

ASMB7-iKVM

远程管理卡

C8098

第一版

2013 年 5 月发行

免责声明

本用户手册是以“现状”及“以目前明示的条件下”的状态提供给您。在法律允许的范围内，华硕就本用户手册，不提供任何明示或默示的担保及保证，包括但不限于商业畅销性、特定目的适用性、未侵害任何他人权利及任何使用本用户手册或无法使用本用户手册的保证，且华硕对因使用本用户手册而获取的结果或通过本用户手册所获得任何信息的准确性或可靠性不提供担保及保证。

用户应自行承担使用本用户手册的所有风险。用户明确了解并同意华硕、华硕的被授权人及董事、管理层、员工、代理商、关联企业皆无须为您因本用户手册、或因使用本用户手册、或因不可归责于华硕的原因而无法使用本用户手册或其任何部分而可能产生的衍生、附带、直接、间接、特别、惩罚或任何其它损失（包括但不限于利益损失、业务中断、资料遗失或其它金钱损失）负责，不论华硕是否被告知发生上述损失之可能性。

由于部分国家或地区可能不允许责任的全部免除或对上述损失的责任限制，所以上述限制或排除条款可能对您不适用。

用户知悉华硕有权随时修改本用户手册。本产品规格或驱动程序一经改变，本用户手册将会随之更新。本用户手册更新的详细说明请您访问华硕的客户服务网http://support.asus.com，或是直接与华硕电脑客户关怀中心 800-820-6655 联系（不能拨打 800 电话的用户，请拨打技术支持电话 021-34074610）。

对于本用户手册中提及的第三方产品名称或内容，其所有权及知识产权都为各产品或内容所有人所有且受现行知识产权相关法律及国际条约的保护。

当下列两种情况发生时，本产品将不再受到华硕的保修及服务：

（1）本产品曾经过非华硕授权的维修、规格更改、零件替换或其它未经过华硕授权的行为。

（2）本产品序号模糊不清或丢失。

注意！倘若本产品上之产品序列号有所破损或无法辨识者，则该项产品恕不保修！

目 录 内 容

第一章：产品介绍

第二章：安装

第三章：华硕主机管理控制器设置

目 录 内 容

第四章：网页用户界面

目录内容

附录：参考信息

安全性须知

电气方面的安全性

- 为避免可能的电击造成严重损害，在搬动电脑主机之前，请先将电脑电源线暂时从电源插槽中拔掉。
- 当您要加入硬件设备到系统中或者要去除系统中的硬件设备时，请务必先连接该设备的数据线，然后再连接电源线。可能的话，在安装硬件设备之前先拔掉电脑电源的电源线。
- 当您要从主板连接或拔除任何的数据线之前，请确定所有的电源线已事先拔掉。
- 在使用扩展卡或扩展卡之前，我们建议您可以先寻求专业人士的协助。这些设备有可能会干扰接地的回路。
- 请确定电源的电压设置已调整到本国/本区域所使用的电压标准值。若您不确定您所属区域的供应电压值为何，那么请就近询问当地的电力公司人员。
- 如果电源已损坏，请不要尝试自行修复。请将之交给专业技术服务人员或经销商来处理。

操作方面的安全性

- 在您安装本产品之前，请务必详加阅读本手册所提供的相关信息。
- 在使用产品之前，请确定所有的排线、电源线都已正确地连接好。若您发现有任何重大的瑕疵，请尽速联络您的经销商。
- 为避免发生电气短路情形，请务必将所有没用到的螺丝、回型针及其他零件收好，不要遗留在主板上或电脑主机中。
- 灰尘、湿气以及剧烈的温度变化都会影响主板的使用寿命，因此请尽量避免放置在这些地方。
- 请勿将电脑主机放置在容易摇晃的地方。
- 若在本产品的使用上有任何的技术性问题，请和经过检定或有经验的技术人员联络。



这个画叉的带轮子的箱子表示这个产品（电子设备）不能直接放入垃圾筒。请根据不同地方的规定处理。

华硕 REACH

注意：请遵守 REACH（Registration，Evaluation，Authorisation，and Restriction of Chemicals）管理规范，我们会将产品中的化学物质公告在华硕 REACH 网站，详细请参考 http://csr.asus.com/english/REACH.htm

关于这本用户手册

　　产品用户手册包含了所有当您在安装华硕 ASMB7-iKVM 远程管理卡时所需用到的信息。

用户手册的编排方式

　　用户手册是由下面几个章节所组成：

- 第一章：产品介绍

  本章节描述本远程管理卡的功能和新技术。

- 第二章：安装

  本章节描述安装管理卡与应用程序。

- 第三章：华硕远程控制程序

  本章节介绍华硕远程控制程序的功能。

- 第四章：网页用户界面

  本章节介绍如何使用网页用户界面来设置与管理服务器。

- 附录：相关信息

  本附录中包含 BMC、LAN 接口信息与疑难解决信息。

提示符号

为了能够确保您正确地完成管理卡设置，请务必注意下面这些会在本手册中出现的标示符号所代表的特殊含意。



警告：提醒您在进行某一项工作时要注意您本身的安全。



小心：提醒您在进行某一项工作时要注意勿伤害到电脑主板元件。



重要：此符号表示您必须要遵照手册所描述之方式完成一项或多项软硬件的安装或设置。



注意：提供有助于完成某项工作的诀窍和其他额外的信息。

哪里可以找到更多的产品信息

您可以通过下面所提供的两个渠道来获得您所使用的华硕产品信息以及软硬件的升级信息等。

1. 华硕网站

您可以到 http://www.asus.com.cn 华硕电脑互联网站取得所有关于华硕软硬件产品的各项信息。

2. 其他文件

在您的产品包装盒中除了本手册所列举的标准配件之外，也有可能会夹带有其他的文件，譬如经销商所附的产品保证单据等。



电子信息产品污染控制标示：图中之数字为产品之环保使用期限。仅指电子信息产品中含有的有毒有害物质或元素不致发生外泄或突变从而对环境造成污染或对人身、财产造成严重损害的期限。

有毒有害物质或元素的名称及含量说明标示：

部件名称	有害物质或元素					
	铅 (Pb)	汞 (Hg)	镉 (Cd)	六价铬 (Cr(VI))	多溴联苯 (PBB)	多溴二苯醚 (PBDE)
印刷电路板及其电子组件	×	○	○	○	○	○
外部信号连接头及线材	×	○	○	○	○	○
外壳	×	○	○	○	○	○
软驱	×	○	○	○	○	○
电池	×	○	○	○	○	○
光驱	×	○	○	○	○	○
散热设备	×	○	○	○	○	○
电源适配器	×	○	○	○	○	○
硬盘	×	○	○	○	○	○
中央处理器与内存	×	○	○	○	○	○

○：表示该有毒有害物质在该部件所有均质材料中的含量均在 SJ/T 11363-2006 标准规定的限量要求以下。

×：表示该有毒有害物质至少在该部件的某一均质材料中的含量超出 SJ/T 11363-2006 标准规定的限量要求，然该部件仍符合欧盟指令 2002/95/EC 的规范。

备注：

1. 此产品所标示之环保使用期限，系指在一般正常使用状况下。
2. 此部件名称涵盖所有服务器相关产品，依产品不同实际涵盖项目会有所减少。

ASMB7-iKVM 规格列表

芯片组	Aspeed 2300
内置 RAM	系统：224MB 视频：32MB
内置 ROM	32 MB
计时器	32-bit Watchdog Timer
主要功能	兼容 IPMI 2.0 支持 KVM over LAN 支持网页用户界面（远程管理） 支持虚拟媒体（Virtual media） 支持 Network Bonding
尺寸	22 mm x 17 mm

* 规格若有任何更改，恕不另行通知。

您可以在本章节中发现诸多华硕所赋予本产品的优异特色，利用简洁易懂的说明，让您能很快的掌握本产品的各项特性，当然，在本章节我们也会提及所有能够应用在本产品的新技术。

1 产品介绍

1.1 欢迎加入华硕爱好者的行列！

再次感谢您购买此款华硕 ASMB7-iKVM 远程管理卡。

华硕 ASMB7-iKVM 兼容智能平台管理接口（Intelligent Platform Management Interface，IPMI）2.0，允许您通过本地网络（LAN）中的中心服务器来监控、控制与管理一台远程服务器。将 ASMB7-iKVM 管理卡插入服务器主板，就可以即时有效地监控服务器。此方案帮助您降低 IT 管理成本，也提高了工作效率。

在您拿到本产品包装盒之后，请马上检查下面所列出的各项标准配件是否齐全。

1.2 产品包装

请检查下面所列出的各项标准配件是否齐全。

- 华硕 ASMB7-iKVM 远程管理卡
- 驱动程序与应用程序光盘
- 用户手册



若以上列出的任何一项配件有损坏或是短缺的情形，请尽快与您的经销商联系。

1.3 功能介绍

1. IPMI 2.0
    - 系统接口（KCS）
    - LAN 接口（支持 RMCP+）
    - 系统事件日志（SEL）
    - 传感数据记录（SDR）
    - 现场可更换部件（FRU）
    - 远程开机/关机，远程重启系统
    - Serial Over LAN（SOL）
    - 验证类型：RAKP-HMAC-SHA1
    - 加密（AES）
    - 事件过滤平台（PEF）
    - 平台事件陷阱（PET）
    - 看门狗计时器（Watchdog Timer）
2. Private I2C 总线
    - 自动监控器（温度、电压、风扇速度与记录事件）
3. PMBus*
    - 支持 PMBus 设备电源
4. PSMI*
    - 支持 PSMI 总线设备电源
5. 网页用户界面
    - 监控器，显示 SDR、SEL、FRU、设置 BMC、LAN
    - 支持 SSL（HTTPS）
    - 多级用户许可
    - 升级 BMC 固件
6. 固件升级
    - DOS 工具
    - 网页图形用户界面（Windows® XP/Vista/2003/2008、RHEL5.2、SLES10SP2）

7. 提示
    - PET
    - SNMP Trap
    - e-Mail
8. KVM over Internet
    - 网页远程控制
9. 远程更新 BIOS
    - 使用远程软驱更新 BIOS
10. 远程存储（虚拟媒体）
    - 支持两个远程存储器，用于 USB/CD-ROM/DVD 与影像
11. 远程安装操作系统
    - 使用远程存储器远程安装操作系统

* 须支持 PMBus 与 PSMI

** 规格若有变更，恕不另行通知

1.4 系统需求

在安装 ASMB7-iKVM 远程管理卡之前，请先确认远程服务器系统是否达到下列要求：

- 支持底板管理控制器（Baseboard Management Controller，BMC）插座*的华硕服务器主板
- 支持 RJ-45 网络接口，用于服务器管理**
- Microsoft® Internet Explorer 5.5 或更新版本；Firefox



* 请访问华硕网站（http://www.asus.com.cn）获取最新支持 ASMB7-iKVM 的服务器主板列表。

** 详细信息请参看附录。

1.5 网络设置

安装在远程服务器主板上的 ASMB7-iKVM 远程管理卡通过直接 LAN 连接或网络集线器连接到本地 / 中心服务器。以下是支持的服务器管理设置：

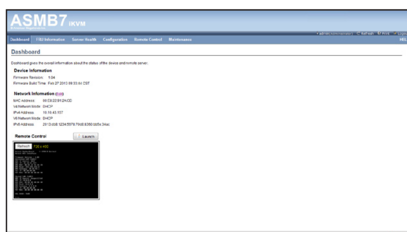
直接 LAN 连接

RJ-45 网线



安装 ASMB7-iKVM 的远程服务器

通过网页浏览器进行远程控制



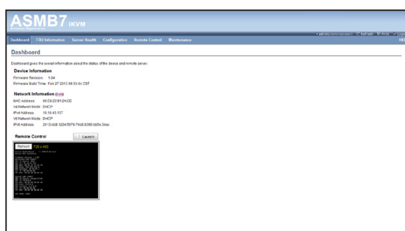
通过网络集线器的 LAN 连接

集线器或路由器



安装 ASMB7-iKVM 的远程服务器

通过网页浏览器进行远程控制



本章节描述了如何将管理卡安装到服务器主板上，并介绍了如何安装各项应用程序。

2 安装

2.1 安装前

在您动手安装远程管理卡到服务器主板上之前，请务必先作好以下所列出的各项预防措施。

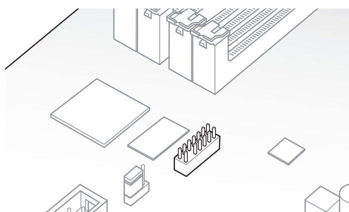


- 在处理服务器主板上的任何元件时，请先拔掉系统的电源线。
- 为避免产生静电，在拿取任何电脑元件时除了可以使用防静电手环之外，您也可以触摸一个有接地线的物品或者金属物品像电源供应器外壳等。
- 拿取集成电路元件时请尽量不要触碰到元件上的芯片。
- 在您移除任何一个集成电路元件后，请将该元件放置在绝缘垫上以隔离静电，或者直接放回该元件的绝缘包装袋中保存。
- 在您安装或移除任何元件之前，请确认电源供应器的电源开关是切换到关闭（OFF）的位置，而最安全的做法是先暂时拔出电源供应器的电源线，等到安装/移除工作完成后再将之接回。如此可避免因仍有电力残留在系统中而严重损及主板、外围设备、元件等。

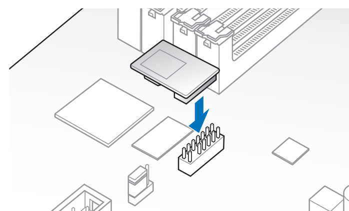
2.2 硬件安装

请依照以下步骤安装远程管理卡：

1. 找到管理卡的 ASMB 插座，将主板上的接针插入 ASMB 插座。



2. 按下管理卡，让插座和接针连接牢固。





主板截图仅供参考。主板类型不同则外观也稍有不同，但是安装步骤保持一致。

3. 紧紧按压主板直到完全安装好。
4. 将网线插入 LAN 接口，以进行服务器管理。



LAN 接口的位置，请参考附录说明。

5. 若要直接连接 LAN，请将网线的另一端插入本地 / 中心服务器的 LAN 接口。

   若要通过网络集线器或路由器连接，请将网线的另一端插入集线器或路由器。
6. 确认 VGA、USB、PS/2 线缆都正确连接。然后将电源插头插入电源插座。



每次插入 AC 电源后，请等待 70 秒后再启动系统。

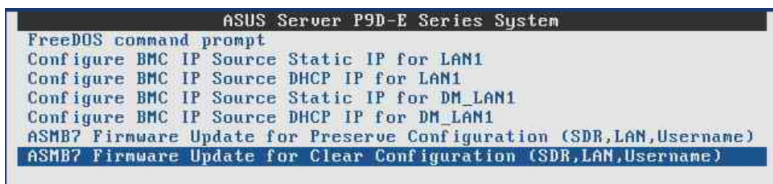
2.3 固件升级与 IP 设置

在开始使用 ASMB7-iKVM 管理卡之前，您需要升级 ASMB7-iKVM 的固件并设置 IP。

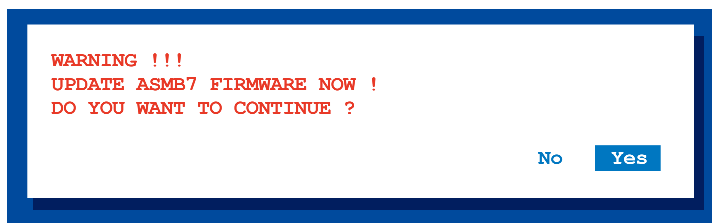
2.3.1 固件升级

请依照以下步骤升级固件：

1. 将驱动程序与应用程序光盘放入光驱。
2. 重启服务器，然后在开机自检（POST）时按下 <Del>，进入 BIOS 设置。
3. 进入“Boot”菜单，将【Boot Device Priority】项目设为 [CD-ROM]。
4. 完成后按下 <F10>，保存设置并退出 BIOS 设置。
5. 重启时，会出现主菜单。选择【ASMB7-iKVM Firmware Update for Preserve Configuration】，然后按下 <Enter> 进入子菜单。



6. 此时会出现一条警告信息，询问您是否确定要升级固件，选择 【Yes】进行升级。



开始升级固件。

7. 当升级完成后，会出现以下画面。

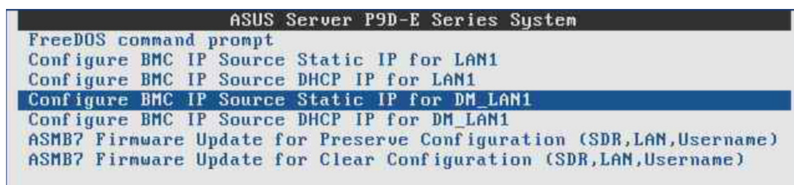
```
Preserving Env Variables...            done
Uploading Firmware Image : 100%... done
Flashing  Firmware Image : 100%... done
Verifying Firmware Image : 100%... done
Setting Env variables ...          done
Resetting the firmware..........
Please wait for 70 seconds to initialize firmware
Delay     70 Seconds
Press any key to continue . . ._
```



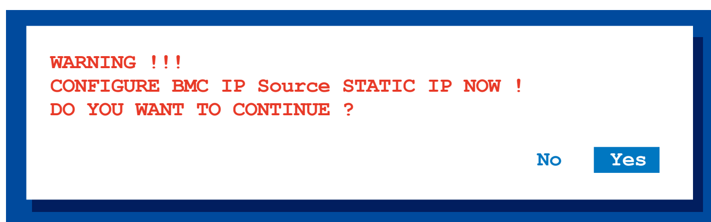
您可以通过网页用户界面来升级固件。请参考 4-13 的详细说明。

2.3.2 设置 BMC IP 源静态 IP

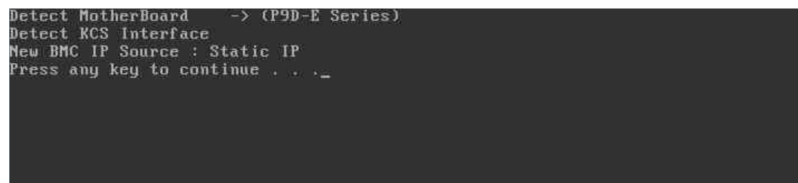
1. 重复上一节中的步骤 1-4。
2. 重启时，会出现主菜单。选择【Configure BMC IP Source Static IP for LAN1（或 DM_LAN1）】，按下 <Enter> 进入子菜单。



3. 此时会出现一条警告信息，询问您是否确定要设置 BMC IP 源静态 IP，选择【Yes】继续。



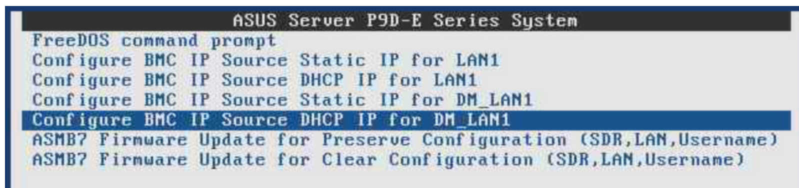
4. 设置完成后，会出现以下画面。



5. 进入 BIOS 菜单设置 IP。请参考“2.4 BIOS 设置”部分 IP 设置的说明。

2.3.3 设置 BMC IP 源 DHCP

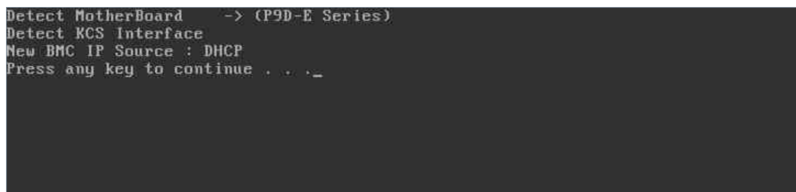
1. 重复上一节中的步骤 1-4。
2. 重启时，会出现主菜单。选择【Configure BMC IP Source DHCP for LAN1（或 DM_LAN1）】，按下 <Enter> 进入子菜单。



3. 此时会出现一条警告信息，询问您是否确定要设置 BMC IP 源 DHCP，选择【Yes】继续。



4. 设置完成后，会出现以下画面。



5. 然后您就可以从 DHCP 服务器取得 IP。

2.4 BIOS 设置

您需要调整远程服务器的 BIOS 设置来连接中心服务器。



- 请根据主板用户手册里的说明来升级远程服务器的 BIOS。请访问华硕网站（http://www.asus.com.cn）来下载主板最新的 BIOS 文件。
- 本章中的 BIOS 设置画面仅供参考，可能与您所见到的画面有所差异。

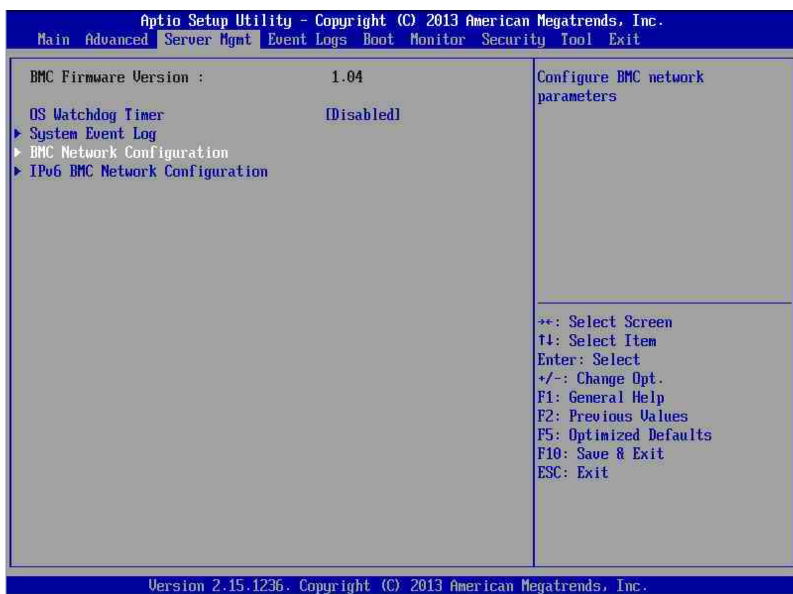
2.4.1 设置 BIOS BMC

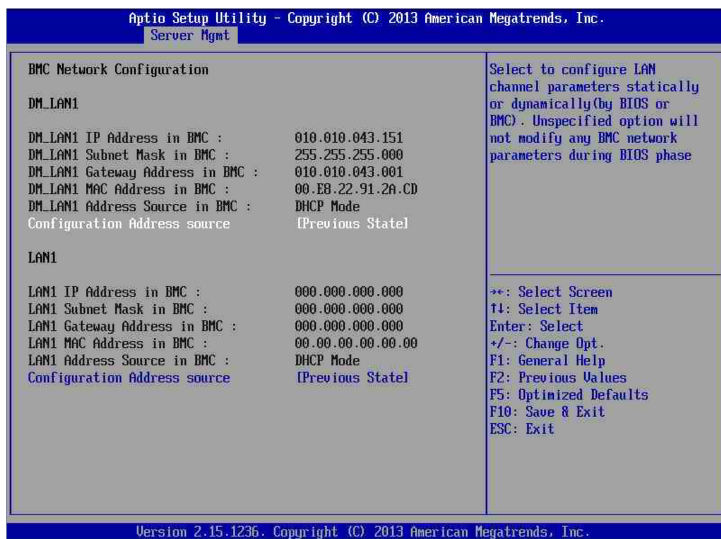
请依照以下步骤设置 BMC：

1. 重启远程服务器，然后在开机自检（POST）时按下 <Del>，进入 BIOS 设置。
2. 进入“Server Mgmt”菜单，选择【BMC network configuration】子菜单。使用此菜单设置 BMC。
3. 完成后，按下 <F10>，保存设置并退出 BIOS 设置。

2.4.2 BMC 网络设置

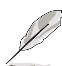
此菜单中的选项用来设置 BMC LAN 参数。





Configuration Source [Previous State]

本项目用来选择 IP 地址源类型。静态或动态设置 LAN 通道参数。



仅当【Configuration Source】项目设为 [Static] 时，以下项目才会出现。

Station IP Address

本项目用来设置 BMC IP 地址。

Subnet Mask

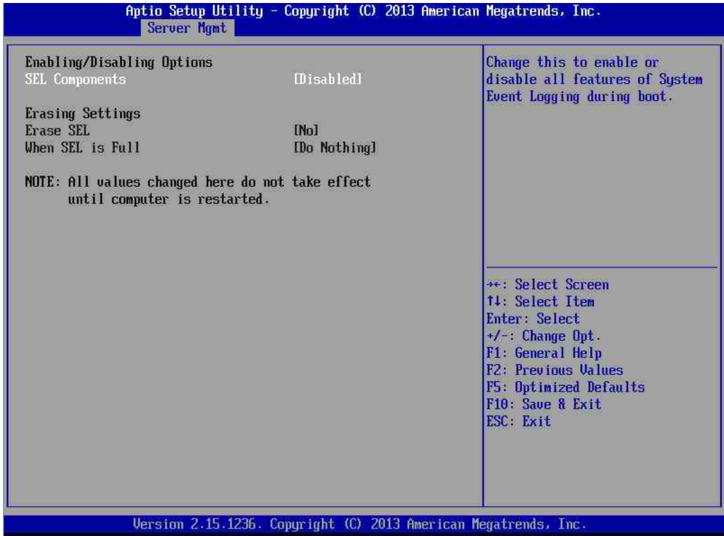
本项目用来设置 BMC 子网掩码。建议您设置与操作系统的网络相同的子网掩码。

Gateway IP Address

本项目用来设置闸道器 IP 地址。

2.4.3 系统事件日志

本项目允许您查看 BMC 事件日志中的所有事件。读取所有 BMC SEL 记录最多会花费 15 秒钟时间。



SEL Components [Disabled]

本项目用来开启或关闭启动时系统事件日志的所有功能。



仅当【SEL Component】项目设为 [Enabled] 时，以下项目才会出现。

Erase SEL [No]

本项目用来选择如何清除 SEL。设置值有：[No] [Yes, On next reset] [Yes, On every reset]

When SEL is Full [Do Nothing]

本项目用来选择您要对全部 SEL 作何操作。设置值有：[Do Nothing] [Erase Immediately]

2.4.4 IPv6 BMC Network Configuration

本项目显示网络频道参数并允许您进行 IPv6 BMC 网络设置。

```
            Aptio Setup Utility - Copyright (C) 2011 American Megatrends, Inc.
   Main  Advanced  Server Mgmt  Event Logs  Boot  Monitor  Security  Tool  Exit

  BMC Firmware Version :                 1.08                Configure IPv6 BMC network
                                                             parameters
  OS Watchdog Timer                      [Disabled]
  OS Wtd Timer Timeout                   [10 minutes]
  OS Wtd Timer Policy                    [Reset]
▶ System Event Log
▶ BMC Network Configuration
▶ IPv6 BMC Network Configuration
```

```
            Aptio Setup Utility - Copyright (C) 2011 American Megatrends, Inc.
                              Server Mgmt

  IPv6 BMC Network Configuration                          Select to configure LAN
                                                          channel parameters statically
                                                          or dynamically(by BIOS or BMC)
  IPv6 BMC DM_LAN1:

  DM_LAN1 IP Address in BMC :
   ->                   2002:DB8:0:F101:0:0:0:1398
  DM_LAN1 Prefix Length in BMC :        64
  DM_LAN1 Gateway Address in BMC :
   ->                   0:0:0:0:0:0:0:0
  DM_LAN1 MAC Address in BMC :          00.E0.18.85.0C.30
  DM_LAN1 Address Source in BMC :       DHCP Mode
  IPv6 BMC DM_LAN1 IP Address Source    [Previous State]
                                                          ←→: Select Screen
  IPv6 BMC Lan1:                                          ↑↓: Select Item
                                                          Enter: Select
  Lan1 IP Address in BMC :                                +/-: Change Opt.
   ->                   2002:DB8:0:F101:0:0:31:4049       F1: General Help
  Lan1 Prefix Length in BMC :           100               F2: Previous Values
  Lan1 Gateway Address in BMC :                           F5: Optimized Defaults
   ->                   0:400:0:0:0:B0A1:3940:0           F10: Save & Exit
  Lan1 MAC Address in BMC :             00.00.00.00.00.00 ESC: Exit
  Lan1 Address Source in BMC :          DHCP Mode
  IPv6 BMC Lan1 IP Address Source       [Previous State]

            Version 2.14.1219. Copyright (C) 2011 American Megatrends, Inc.
```

IPv6 BMC DM_LAN1 IP Address Source [Previous State]

可让您选择 IP 地址来源类型并动态设置网络频道参数。设置值有：[Previous State] [Static] [Dynamic-Obtained by BMC running DHCP]



仅当 IPv6 BMC DM_LAN1 IP 地址来源设置为 [Static] 时下列选项才会出现。

IPv6 BMC DM_LAN1 IP Address

可设置 IPv6 BMC DM_LAN1 IP 地址。

IPv6 BMC DM_LAN1 IP Prefix Length

可设置 IPv6 BMC DM_LAN1 IP Prefix 长度。

IPv6 BMC DM_LAN1 Default Gateway

可设置 IPv6 BMC DM_LAN1 Gateway IP 地址。

IPv6 BMC Lan1 IP Address Source [Previous State]

可让您选择 IP 地址来源类型并动态设置网络频道参数。设置值有：[Previous State] [Static][Dynamic-Obtained by BMC running DHCP]



仅当 IPv6 BMC Lan1 IP 地址来源设置为 [Static] 时下列选项才会出现。

IPv6 BMC Lan1 IP Address

可设置 IPv6 BMC Lan1 IP 地址。

IPv6 BMC Lan1 IP Prefix Length

可设置 IPv6 BMC Lan1 IP Prefix 长度。

IPv6 BMC Lan1 Default Gateway

可设置 IPv6 BMC Lan1 Gateway IP 地址。

2.5 运行 ASMC7 应用程序

您可以使用 ASMC7 程序来升级 ASMB7-iKVM 固件、为远程服务器设置 LAN，并可在 DOS 环境下变更用户名 / 密码。驱动程序与应用程序光盘中包含此程序。

请依照以下步骤运行 ASMC7 应用程序：

1. 将驱动程序与应用程序光盘放入光驱。
2. 重启远程服务器，然后在开机自检（POST）时按下 <Del>，进入 BIOS 设置。
3. 进入 "Boot" 菜单，将【Boot Device Priority】项目设为 [CD-ROM]。
4. 完成后按下 <F10>，保存设置并退出 BIOS 设置。
5. 重启时，会出现主菜单。选择【FreeDOS command prompt】 然后按下 <Enter> 进入子菜单。

```
                 ASUS Server P9D-E Series System
 FreeDOS command prompt
 Configure BMC IP Source Static IP for LAN1
 Configure BMC IP Source DHCP IP for LAN1
 Configure BMC IP Source Static IP for DM_LAN1
 Configure BMC IP Source DHCP IP for DM_LAN1
 ASMB7 Firmware Update for Preserve Configuration (SDR,LAN,Username)
 ASMB7 Firmware Update for Clear Configuration (SDR,LAN,Username)
```

6. 当出现 C:> 提示符时，输入 ASMC7 -?，然后按下 <Enter> 来显示 ASMC7 程序帮助菜单。画面如下图所示。

```
+-----------------------------------------------------------+
| ASUS Server Management Card Utility 7.00 Help Menu        |
+-----------------------------------------------------------+
Usage:
ASMC7 -kcs[smic/bt/pci_smic] NetFn command data....
ASMC7 -bmc_ip_source source[1:Static, 2:DHCP]
ASMC7 -bmc_ip ip_addr[10.10.10.20]
ASMC7 -bmc_mask ip_mask[255.255.255.0]
ASMC7 -bmc_gateway ip_addr[10.10.10.254]
ASMC7 -ipv6_source source[1:Static, 2:DHCP]
ASMC7 -ipv6 ipv6_addr[2001:0db8:1234:5678:8769:e1cb:aabb:ccdd]
ASMC7 -ipv6_prefix prefix_length[64]
ASMC7 -pet_ip_mac ip_addr[10.10.10.20] mac_addr[010203040506]
ASMC7 -bmc_ip_s_lan1 source[1:Static, 2:DHCP]
ASMC7 -bmc_ip_lan1 ip_addr[10.10.10.20]
ASMC7 -bmc_mask_lan1 ip_mask[255.255.255.0]
ASMC7 -bmc_g_lan1 ip_addr[10.10.10.254]
ASMC7 -ipv6_s_lan1 source[1:Static, 2:DHCP]
ASMC7 -ipv6_lan1 ip_addr[2001:0db8:1234:5678:8769:e1cb:aabb:ccdd]
ASMC7 -ipv6_pre_lan1 prefix_length[64]
ASMC7 -pet_ip_m_lan1 ip_addr[10.10.10.20] mac_addr[010203040506]


<Press any key to see the next page> <ESC key to break>_
```

按任意键查看下一页。

```
<Press any key to see the next page> <ESC key to break>
ASMC7 -adm_name new_name_string
ASMC7 -user_name new_name_string
ASMC7 -adm_password new_adm_password
ASMC7 -user_password new_user_password
ASMC7 -sol_baud 57600[9600/19200/38400/57600/115200]
ASMC7 -bmc_info
ASMC7 -fru -view fru_id
ASMC7 -fru -load fru_file
ASMC7 -fru -save fru_id fru_file
ASMC7 -sel -clear
C:\>
```

ASMC7 帮助菜单项目说明

项目	描述
-kcs[smic/bt/pci_smic] NetFn command data....	发送 IPMI 指令
-bmc_ip_source source[1: Static, 2: DHCP]	设置 IP 源
-bmc_ip [ip_addr] (e.g., bmc_ip 10.10.10.20)	写入独立 LAN 的 BMC IP 地址
-bmc_mask [ip_mask] (e.g., bmc_mask 255.255.255.0)	写入独立 LAN的子网掩码
-bmc_gateway [ip_addr] (e.g., bmc_gateway 10.10.10.254)	写入独立 LAN 的网关地址
-pet_ip_mac [ip_addr] [mac_addr] (e.g., pet_ip_mac 10.10.10.20 010203040506)	写入独立 LAN 的 PET 目标 IP 与 MAC 地址
-bmc_ip_s_lan1 source[1: Static, 2: DHCP]	设置共享 LAN 的 IP 源
-bmc_ip_lan1 [ip_addr] (e.g., bmc_ip 10.10.10.20)	写入共享 LAN 的 BMC IP 地址
-bmc_mask_lan1 [ip_mask] (e.g., bmc_mask 255.255.255.0)	写入共享 LAN 的子网掩码
-bmc_g_lan1 [ip_addr] (e.g., bmc_gateway 10.10.10.254)	写入共享 LAN 的网关地址
-pet_ip_m_lan1 [ip_addr] [mac_addr] (e.g., pet_ip_mac 10.10.10.20 010203040506)	写入共享 LAN 的 PET 目标 IP 与 MAC 地址
-adm_name new_name_string	变更管理名
-user_name new_name_string	变更用户名
-adm_password new_adm_password	变更管理密码
-user_password new_user_password	变更用户密码
-sol_baud [baud rate] (e.g., sol_baud 57600)	设置通讯波特率
-bmc_info	显示 BMC 与 PET IP 与 MAC 地址
-fru -view fru_id	显示系统 FRU 信息
-fru -load fru_file	从文件更新系统 FRU 数据
-fru -save fru_id fru_file	保存系统 FRU 数据到文件中
-sel -clear	清除系统事件日志

2.5.1 设置 LAN 控制器

在连接 ASMB7-iKVM 管理卡之前，您必须设置LAN 接口，以便让远程服务器连接到本地 / 中心服务器。

请依照以下步骤设置远程服务器的 LAN 接口：

1. 根据前面部分的说明，运行驱动程序与应用程序光盘中的 ASMC7 应用程序。
2. 设置 IP 源：
   (a) 若要设置静态 IP 地址，请输入 ASMC7 -bmc_ip_source 1。
   (b) 若要从 DHCP 服务器取得 IP，请输入 ASMC7 -bmc_ip_source 2。
3. 输入 ASMC7 -bmc_ip xxx.xxx.xxx.xxx，然后按下 <Enter>为远程服务器 LAN 接口指定任何 IP 地址（若有需要）。屏幕会显示指令与回应缓冲。请将远程服务器的 IP 地址写下来供以后参考。

```
c:\>ASMC7 -bmc_ip  10.10.10.243
Detect MotherBoard     -> (Z9PE-D16 Series)
Detect KCS Interface
New BMC IP : 10.10.10.243
c:\>
```

完成后，回到 DOS 画面。



请确认远程与本地 / 中心服务器的 IP 地址在同一个子网内。您可以使用操作系统中的网络设置程序来进行确认。

4. 若有需要，请设置（a）子网掩码与（b）网关地址。
   (a) 输入 ASMC7 -bmc_mask xxx.xxx.xxx.xxx（您的子网掩码在十进制系统中编译）。
   (b) 输入 ASMC7 -bmc_gateway xxx.xxx.xxx.xxx（您的网关地址在十进制系统中编译）。
5. 重启远程服务器，进入 BIOS 设置，然后从硬盘启动。
6. 若有需要，请调整本地 / 中心服务器的网络设置。

2.5.2 设置用户名与密码

您可以使用 ASMC7 应用程序变更用户名与密码。

请依照以下步骤变更用户名与密码：

1. 执行 2-11 页的步骤 1-5。
2. 当 C:> 提示符出现时，输入 ASMC7 -user_name xxxxx，然后按下 ＜Enter＞ 变更用户名。

```
C:\>ASMC7 -user_name super
Detect MotherBoard     -> (Z9PE Series)
Detect KCS Interface

Change User Name to super
C:\>
```

3. 输入 ASMC7 -user_password xxxxxxxx 然后按下 ＜Enter＞ 变更密码。
4. 重启远程服务器，进入 BIOS 设置，然后从硬盘启动。

本章介绍如何设置服务器主板所支持的华硕主机管理控制器，及如何使用此程序。

3 华硕主机管理控制器设置

3.1 华硕主机管理控制器设置（Host Management Controller Setup）

华硕 Host Management Controller Setup 应用程序能提供准确的设置与基本功能，包括生成 System Event Log（SEL）与 System Data Record (SDR)。

此应用程序也可用于设置主机接口与系统信息的即时监控，包括 CPU 温度、风扇速度与系统电压。

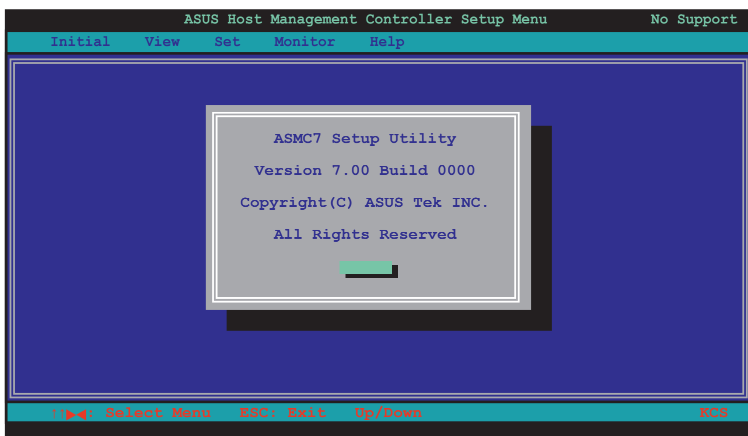
3.1.1 安装并运行华硕 Host Management Controller Setup 应用程序

请依照以下步骤安装华硕 Host Management Controller Setup 应用程序：

1. 用驱动程序与应用程序光盘开机进入 DOS 模式。
2. 在弹出的窗口中，输入 ASMC7，按下 <Enter> 显示 ASMC7 应用程序帮助菜单。画面如下图所示。

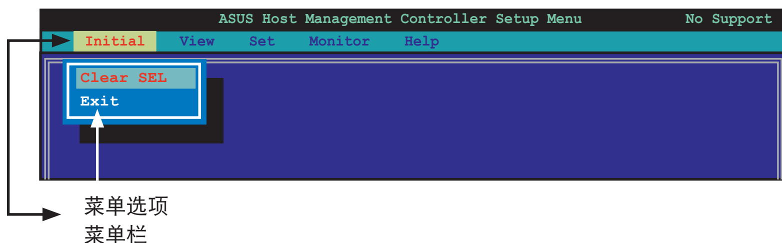
```
C:\>ASMC7
```

3. 程序主画面出现后，按下 <Enter>。



3.1.2 菜单栏

应用程序菜单栏有五个菜单：初始化（Initial）、查看（View）、设置（Set）、监控（Monitor）与帮助（Help）。您可以使用左 / 右方向键进行选择。进入菜单后，使用上 / 下方向键显示设置项目，并按下 <Enter> 进行设置。

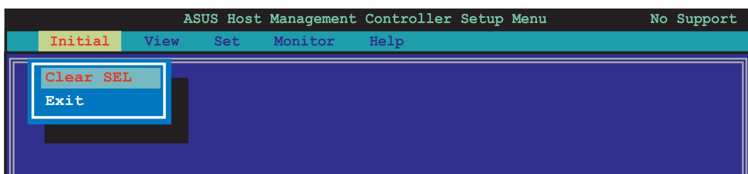


3.1.3 初始化（Initial）

【Initial】选项用于清除 SEL 信息或退出应用程序。

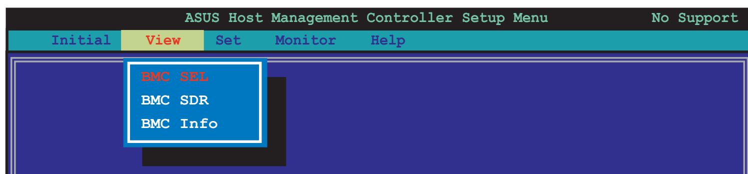
在【Initial】中选择【Clear SEL】清除所有系统事件日志信息。若要创建一个从特定时间开始的新日志用于监控系统，使用【Clear SEL】。

选择【Exit】关闭应用程序，并回到 DOS画面。



3.1.4 查看（View）

【View】选项显示底板管理控制器（BMC）数据记录，包括 System Event Log (SEL)、System Data Record (SDR) 与总体 BMC 信息。

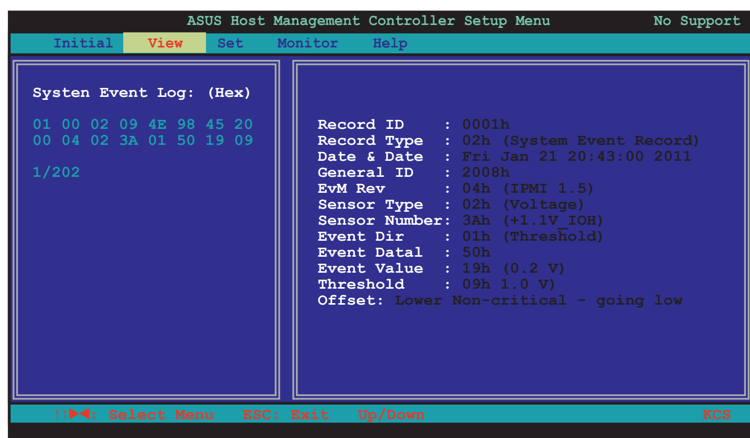


查看系统事件日志（System Event Log，SEL）：

1. 在【View】中选择【BMC SEL】，按下 <Enter>。左边显示系统事件信息。右边显示 SEL 信息。

   窗口左下角的数字表示右边面板显示的事件数与远程主机上系统事件的总数。

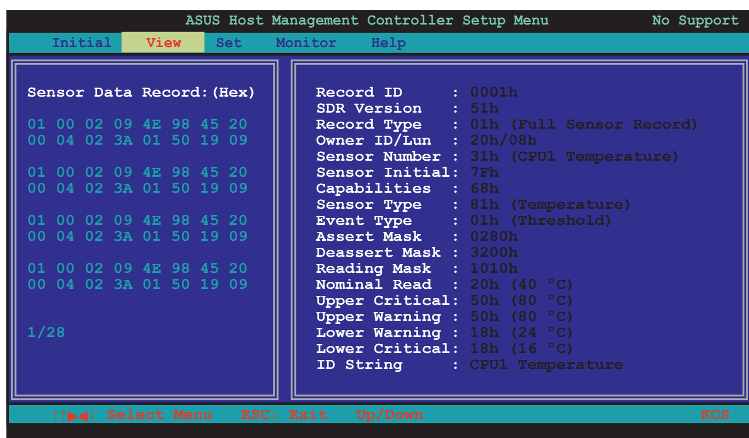
2. 使用向下箭头往下显示下一条监控信息。
3. 完成后按下 <Esc> 回到主画面。



查看系统数据记录（System Data Record，SDR）：

1. 在【View】中选择【BMC SDR】，按下 <Enter>。左边显示所有数据记录。右边显示监控数据信息。

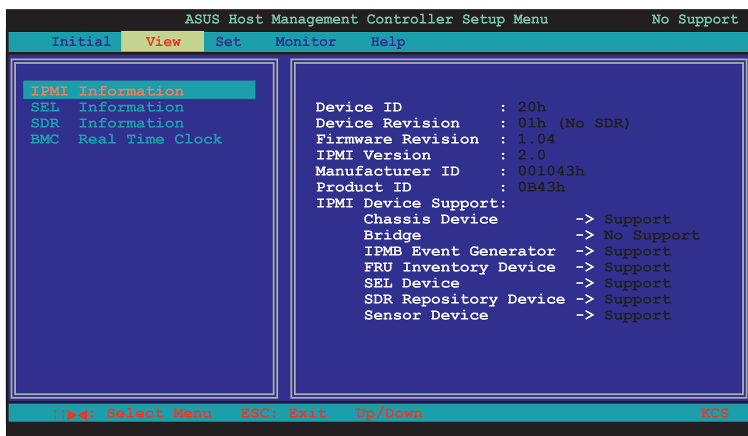
   窗口左下角的数字表示右边面板显示的数据记录与远程主机上监控数据的总数。



2. 使用向下箭头往下显示下一条监控数据记录。
3. 完成后按下 <Esc> 回到主画面。

查看 BMC 信息：

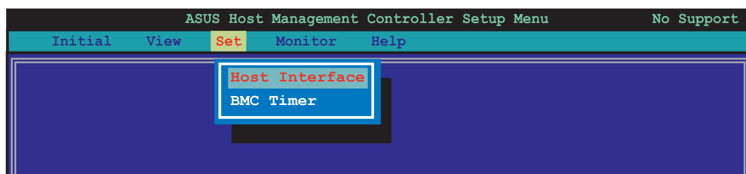
1. 在【View】中选择【BMC Info】，按下 ＜Enter＞。左边显示 BMC 信息。
2. 使用向下箭头选择一条 BMC 信息，右边会显示 BMC 的详细信息。



3. 完成后按下 ＜Esc＞ 回到主画面。

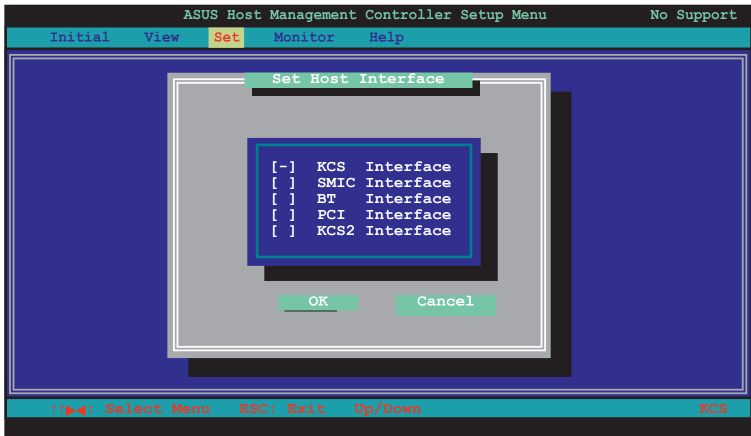
3.1.5 设置（Set）

【Set】选项用于控制主机接口类型与正确的 BMC 时间。



选择主机接口：

1. 在【Set】中选择【Host Interface】，按下 <Enter>。屏幕显示远程管理卡支持主机接口。
2. 使用向下箭头选择主机接口，按下 <Enter>。



您可以选择以下主机接口：

KCS Interface	-	键盘控制型
SMIC Interface	-	服务器管理界面芯片
BT Interface	-	Block Transfer
PCI Interface	-	外围设备内部接口
KCS2 Interface	-	键盘控制型 2

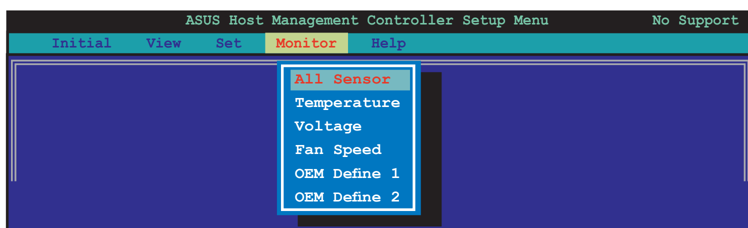
3. 完成后按下 <Esc> 回到主画面。

设置 BMC Timer：

1. 在【Set】中选择【BMC Timer】，按下 <Enter>。
2. 将 BMC IPMI 时钟设置为现在的系统时间。
3. 完成后按下 <Esc> 回到主画面。

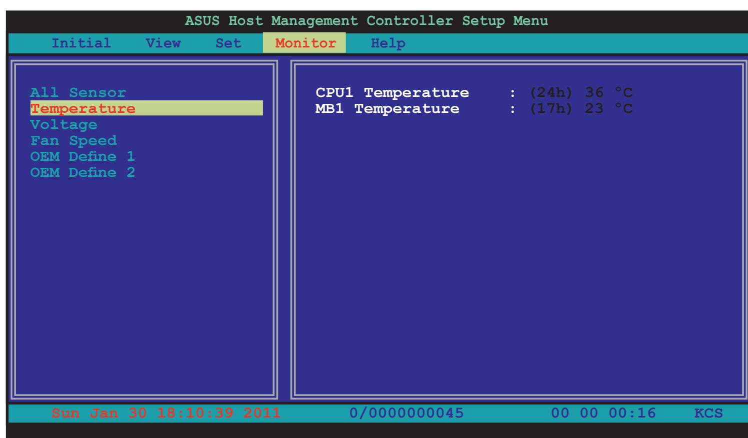
3.1.6 监控（Monitor）

【Monitor】选项显示远程服务器系统的日期与 CPU 温度、电压与风扇速度。



显示远程服务器信息：

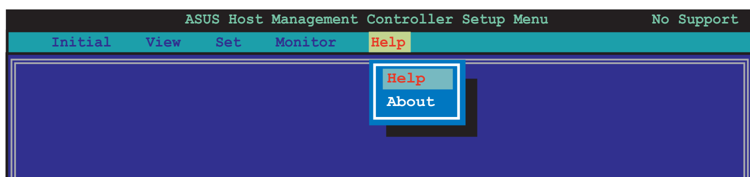
1. 在【Monitor】中选择一个监控器，按下 <Enter>。左边显示服务器信息。
2. 使用向下箭头选择一条监控信息，右边会显示监控的详细信息。



3. 按下 <Esc> 回到主画面。

3.1.7 帮助（Help）

【Help】选项显示应用程序选项、版本与版权等信息。



本章介绍如何使用网页用户界面来设置与管理服务器。

网页用户界面

4

4.1 网页用户界面

网页用户界面可帮助您轻松地监控远程服务器的硬件信息，包括温度、风扇速度、电压与电源。此应用程序也可帮助您快速开启 / 关闭或重置远程服务器。

按照以下步骤进入网页用户界面：

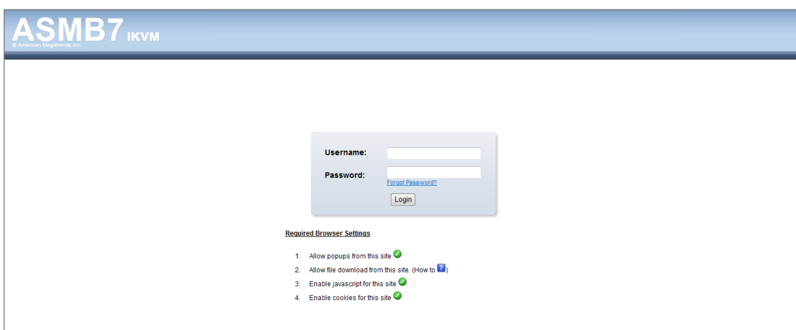
1. 在开机自检（POST）时进入 BIOS 设置程序。
2. 点击 Advanced Menu > Runtime Error Logging > CPU II0 Bridge Configuration > Launch Storage OpROM，然后按下 <Enter>。
3. 将【Launch Storage OpROM】项目设为 [Enabled]。
4. 点击 Mgmt Menu > BMC network configuration > Configuration Address source，然后按下 <Enter>。
5. 输入 IP Address in BMC、Subnet Mask in BMC 与 Gateway Address in BMC。
6. 按下 <F10> 保存更改并退出 BIOS 设置程序。



在使用此网页管理程序前，请在远程服务器上安装 JRE。您可以在 ASMB7-iKVM 的驱动程序与应用程序光盘中的 JAVA 文件夹中找到 JRE 应用程序。您也可以访问 http://www.oracle.com/technetwork/java/javase/downloads/index.html 来下载 JRE。

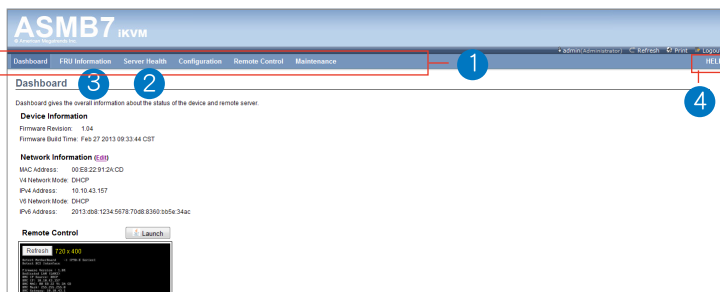
4.1.1 登录应用程序

1. 请确认电脑的网线连接到远程服务器的 LAN 接口中。
2. 打开网页浏览器，输入与远程服务器相同的 IP 地址。
3. 此时出现以下画面。输入默认的用户名（admin）和密码（admin）。然后点击【Login】（登录）。



4.1.2 使用应用程序

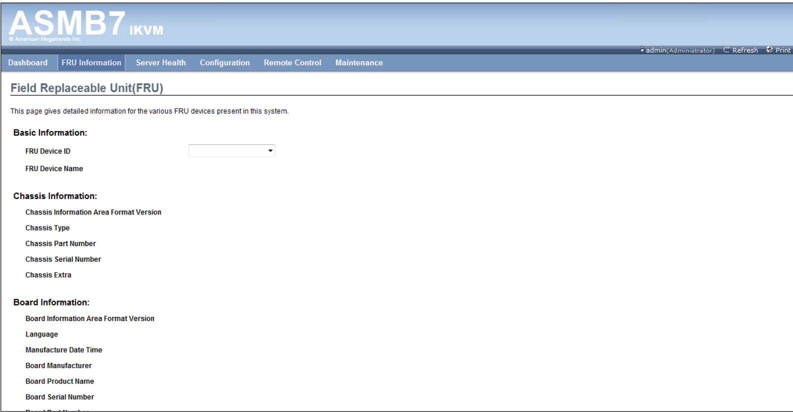
当您成功登录后，网页图形用户界面将出现。



1. 菜单栏：点击菜单显示此菜单下的功能列表。
2. 功能列表：点击每个功能键开始使用这一功能。
3. 功能名称：显示功能名称。
4. 帮助菜单：点击此处显示所选功能的简要说明。

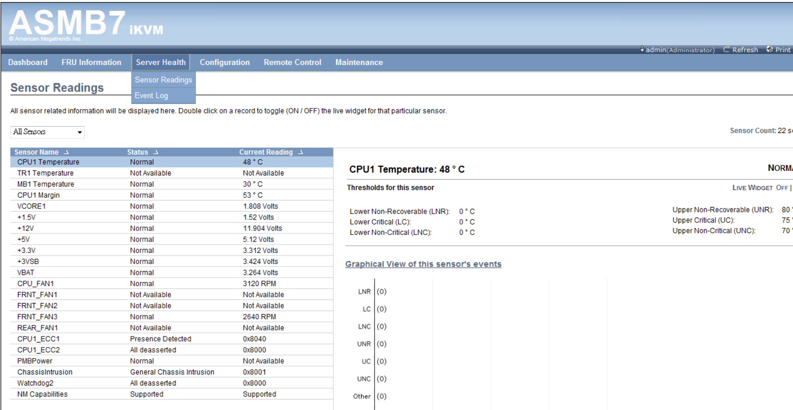
4.2 系统信息（FRU Information）

此部分介绍系统中各个 FRU 设备的信息概况。



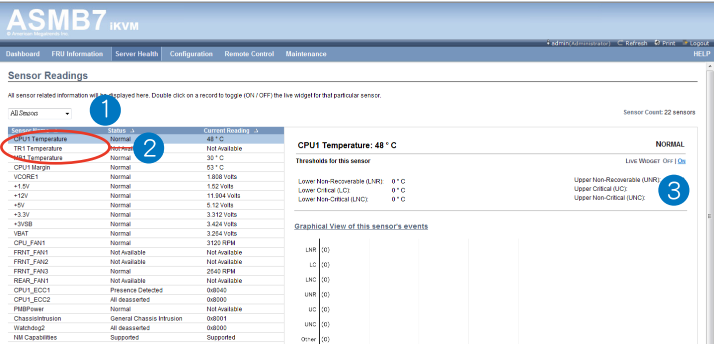
4.3 服务器状况（Server Health）

此部分显示与服务器状况相关的数据，如监控器信息与事件日志。点击每个选项查看此选项的信息。



4.3.1 监控信息 (Sensor Readings (with Thresholds))

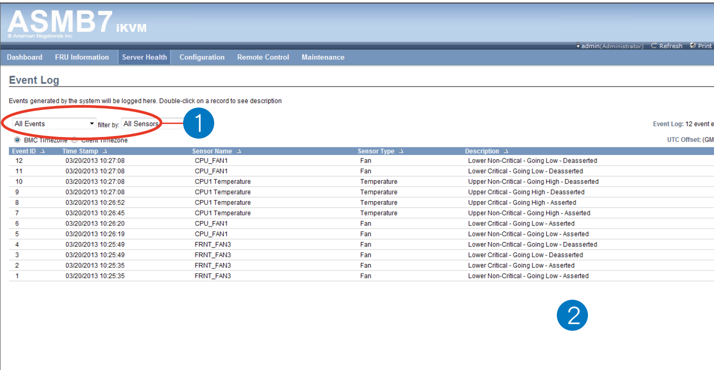
Sensor Readings 页面显示系统监控器信息，包括监控值与监控状态。



1. Select a sensor type category：允许您选择要显示的监控信息类型
2. Status List：选择您在下拉列表中选择的监控信息列表类型。
3. Live Widget：点击以开启或关闭 Live Widget 功能。

4.3.2 事件日志（Event Log）

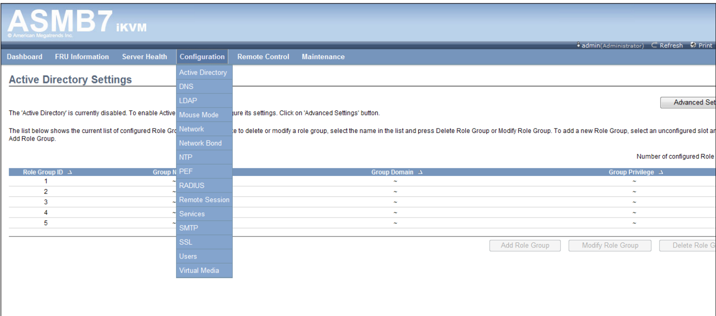
Event Log 页面显示系统事件日志。



1. Select an event log category：允许您选择要显示的事件类型
2. Clear Event Log：点击清除事件日志

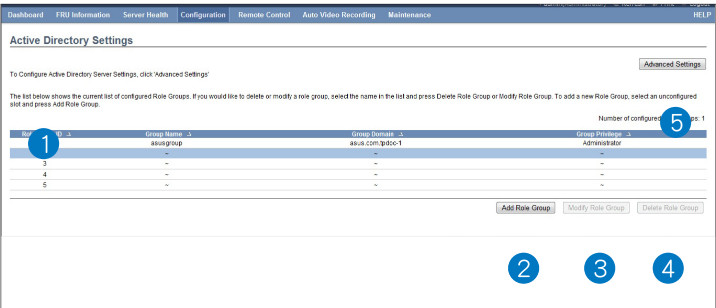
4.4 设置（Configuration）

此部分用于对系统进行设置。点击每个选项开始进行设置。



4.4.1 活动目录（Active Directory）

Active Directory 拥有多项功能，包括提供对像信息、组织对像以便更好地进行访问、允许用户与管理员存取、以及允许管理员设置目录安全。要开启 Active Directory 设置页面，从主菜单点击【Configuration】>【Active Directory】。Active Directory 设置页面如下图所示。



1. Role Group ID：用于识别角色组在 Active Directory 中的的名称。角色组名称是一串 255 个数字、字母组成的字串。可使用特殊字符 “- ” 与 “_” 。
2. Add Role Group：添加新的角色组至设备。
3. Modify Role Group：修改角色组。或者，双击要设置的插槽。
4. Delete Role Group：删除已有角色组。
5. Advanced Settings：此项目用来进行 Active Directory 的高级设置。项目有：Enable Active Directory Authentication、User Domain name、Time Out、Domain Controller Server Addresses。

步骤：

按以下步骤在“Advanced Active Directory Settings”页面输入详细信息：

1. 点击【Advanced Settings】打开“Advanced Active Directory Settings”页面。

Advanced Active Directory Settings

Active Directory Authentication	☑ Enable
User Domain Name	asus.com
Time Out	120
Domain Controller Server Address1	10.10.192.2
Domain Controller Server Address2	
Domain Controller Server Address3	

Save Cancel

2. 在“Active Directory Settings”页面，输入以下详细信息。
3. 【Active Directory Authentication】：要开启或关闭 Active Directory，可分别勾选或取消勾选 [Enable]。



若您已开启 Active Directory Authentication，请输入必要的信息以访问 Active Directory 服务器。

4. 在“User Domain Name”区域为用户设置域名。如：asus.com
5. 在“Time Out”区域设置 Active Directory 请求完成的等待时间。



1. 默认超时值：120 秒。
2. 允许范围：15 至 300。

6. 在“Domain Controller Server Address1”、“Domain Controller Server Address2”与“Domain Controller Server Address3”处设置 IP 地址。
7. 点击【Save】保存设置并返回“Active Directory Settings”页面。
8. 点击【Cancel】取消设置并返回“Active Directory Settings”页面。

添加新的角色组（Role Group）

1. 在“Active Directory Settings”页面，选择空白行并点击【Add Role Group】打开添加页面，如下图所示：

Add Role Group

Role Group Name	
Role Group Domain	
Role Group Privilege	Administrator

Add Cancel

2. 在“Role Group Name”区域，输出角色组在 Active Directory 中的识别名称。



1. 角色组名称是一串 255 个字母、数字组成的字符串。
2. 可使用特殊字符“- ”与“_”。

3. 在“Role Group Domain”区域，输入要添加角色组的域名。



1. 域名是一串 255 个字母、数字组成的字符串。
2. 不可使用特殊字符“- ”与“_”。

4. 在“Role Group Privilege”区域，输入该群组的层级。
5. 点击【Add】保存新的角色组并返回角色组列表。
6. 点击【Cancel】取消设置并返回角色组列表。

修改角色组（Role Group）

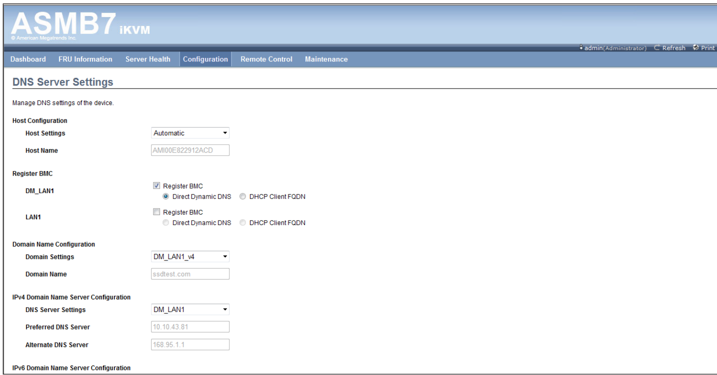
1. 在“Active Directory Settings”页面，选择您要修改的行并点击【Modify Role Group】。
2. 作必要的修改，然后点击【Save】。

删除角色组（Role Group）

在“Active Directory Settings”页面，选择您要删除的行并点击【Delete Role Group】。

4.4.2 DNS

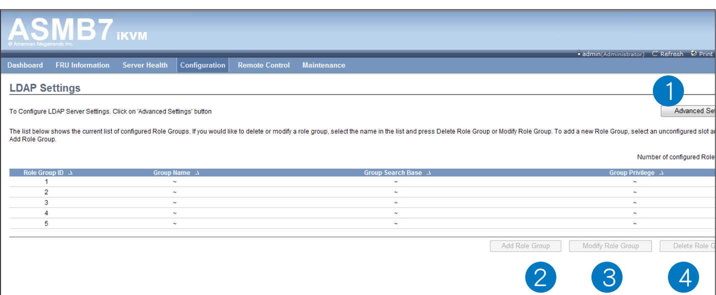
此页面用来管理设备的 DNS 设置。



4.4.3 LDAP

“Lightweight Directory Access Protocol”（LDAP）是一项应用协议，用来查询并修改 Internet Protocol (IP) 网络中的目录服务的日期。若您的网络中有一台已配置的 LDAP 服务器，您可以使用它方便地添加、管理并验证 MegaRAC® 卡用户。这是通过把登录请求转交给 LDAP 服务器来完成的。这也表示当使用 MegaRAC 卡时无需再定义附加的验证机制。因为您现有的 LDAP 服务器保留了验证功能，您时刻知道哪些用户在使用网络资源，并且可以方便地定义用户或群组规则来进行存取控制。

从主菜单点击【Configuration】>【LDAP】来打开 LDAP 设置页面。LDAP 设置页面如下图所示。



1. Advanced Settings：设置 LDAP 高级设置。项目有：Enable LDAP Authentication、IP Address、Port and Search base。

2. Add Role Group：添加一个新的角色组至设备。或者，双击空的插槽来添加角色组。
3. Modify Role Group：修改指定的角色组。
4. Delete Role Group：从列表中删除角色组。

步骤：

在“Advanced LDAP Settings”页面输入详细信息：

1. 在 LDAP 设置页面，点击【Advanced Settings】。LDAP 设置页面如下图所示。

Advanced LDAP Settings

LDAP Authentication	☑ Enable
IP Address	10.10.192.1
Port	389
Bind DN	cn=admin ou=login dc=domain dc=
Password	
Search Base	cn=admin ou=login dc=domain

Save Cancel

2. 要开启或关闭 LDAP Authentication，勾选或取消勾选 [Enable]。



在登录的弹出窗口中，输入用户名以 ldap Group 成员登录。

3. 在“IP Address”区域输入 LDAP 服务器的 IP地址。



1. IP 地址是由 . 分隔的四组数字“xxx.xxx.xxx.xxx”。
2. 每组数字的范围为 0 至 255。
3. 第一组数字必须为 0。
4. 支持 IPv4 地址格式与 IPv6 地址格式。

4. 在“Port”区域设置 LDAP 端口。



默认端口为 389。安全连接默认端口为 636。

5. 输入 Search Base。Search base 告诉 LDAP 服务器搜索外部目录树的哪一部分。search base 与外部目录的组织、群组类似。
6. 点击【Save】保存设置。
7. 点击【Cancel】取消更改。

添加新的角色组

1. 在 LDAP 设置页面，选择空的行并点击【Add Role Group】打开“Add Role group”页面。
2 在“Role Group Name”区域，输入角色组名称。
3. 在“Role Group Search Base”区域，输入角色组的位置路径。



1. Search Base 是一串 255 个数字、字母组成的字串。
2. 不可使用特殊字符“- ”与“__”。

4. 在“Role Group Privilege”区域，输入指定到此群组的权限层级。
5. 点击【Add】保存新的角色组并返回角色组列表。
6. 点击【Cancel】取消设置并返回角色组列表。

修改角色组

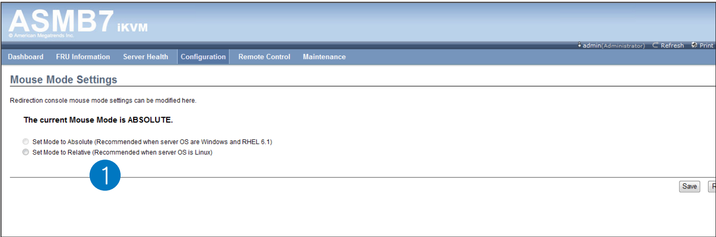
1. 在 LDAP 设置页面，选择您要修改的行，然后点击【Modify Role Group】。
2. 进行修改，然后点击【Save】。

删除角色组

在 LDAP 设置页面，选择您要删除的行，然后点击【Delete Role Group】。

4.4.4 鼠标模式（Mouse Mode）

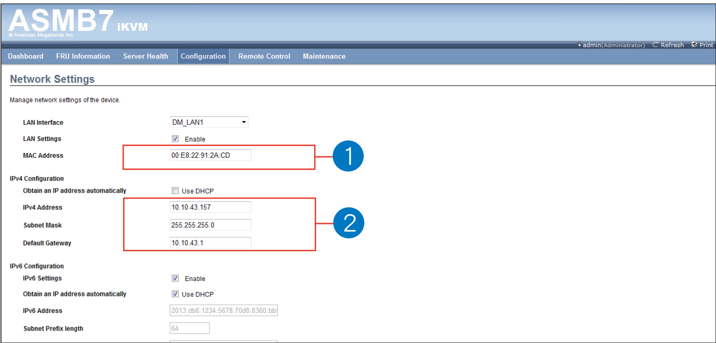
Mouse Mode 页面用于选择鼠标模式。



1. Save：选择想要的鼠标模式，然后点击【Save】保存设置。

4.4.5 网络（Network）

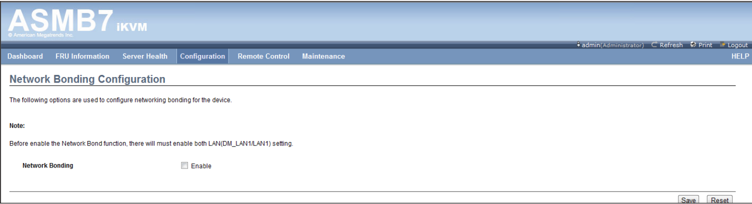
Network 页面用于设置网络。



1. MAC Address：选择自动取得或手动设置 IP。
2. IP Address/Subnet Mask/Default Gateway：若您设置静态 IP，在相关区域内输入 IP 地址、子网掩码与网关。

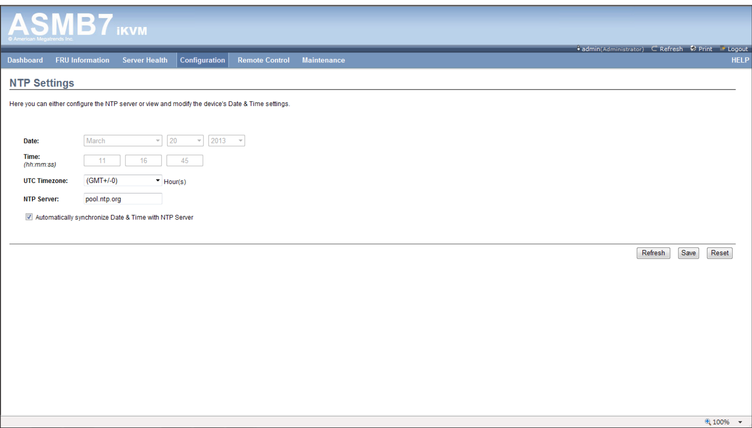
4.4.6 Network Bond

此页面用来开启或关闭 networking bonding 功能，以及设置默认界面。



4.4.7 NTP

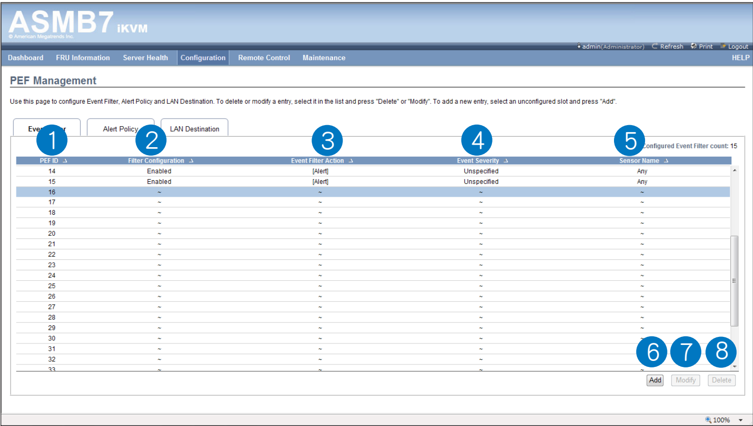
此页面用来设置 NTP 服务器或查看并修改设备的时间与日期设置。



4.4.8 PEF

Platform Event Filtering (PEF) 提供一套机制来设置 BMC 以对它收到的或内部生成的事件信息采取选择性的动作。这些动作包括如系统关机、重启、生成警报等。执行 PEF 需建议在事件过滤表中提供至少 16 个条目。这些条目应先预置以应对常见的系统失败事件，如系统过热、系统启动失败、风扇错误等。

要打开 PEF Management Settings 页面，从主菜单点击【Configurations】>【PEF】。PEF Management Settings 页面如下图所示。



PEF 管理用于设置以下内容：

- Event Filter（事件过滤）
- Alert Policy（警报规则）
- LAN Destination（网络目的地）

Event Filter 标签页

建议您使用 PEF implementation，在事件过滤表中提供至少 16 个条目。这些条目的子集应针对常见的系统失败事件（如过热、供电系统失败、风扇失败等）进行预设。

1. PEF ID：此区域显示新设置的 PEF 条目（只读）事件的 ID。
2. Filter configuration：勾选以开启 PEF 设置。
3. Event Filter Action：勾选以开启 PEF 警报。此项为强制项目。
4. Event Severity：从列表中选择任一事件严重性。
5. Sensor Name：从列表中选择感应器。
6. Add：添加新的事件过滤条目并返回“Event filter”列表。
7. Modify：修改已有条目。
8. Cancel：取消修改并返回“Event filter”列表。

步骤：

1. 点击“Event Filter”标签页在可用的插槽上设置事件过滤器。
2. 要添加事件过滤条目，选择一个空的插槽，然后点击【Add】打开添加事件过滤器页面。如下图所示：

ASMB7 iKVM
© American Megatrends Inc.

Dashboard | FRU Information | Server Health | Configuration | Remote Control | Maintenance

Modify Event Filter entry

Use this page to modify the existing Event Filter entry. Click 'Modify' to accept the modification.

Event Filter Configuration
PEF ID: 1
Filter Configuration: Enable
Event Severity: Information

Filter Action configuration
Event Filter Action: Alert

3. Event Filter Configuration 部分：
- PEF ID 显示设置的 PEF 条目（只读）的 ID。
- 在过滤器设置页面，勾选开启 PEF 设置。
- 在“Event Severity”中选择任一事件严重性。

4. Filter Action configuration 部分：
- Event Filter Action 为强制项目，默认为开启，开启 PEF 警报（只读）。
- 从下拉列表中选择任一电源动作：Power down、Power reset 或 Power cycle。
- 从下拉列表中选择任一已设置的 Alert Policy 号码。



点击【Configuration】->【PEF】->【Alert Policy】设置 Alert Policy。

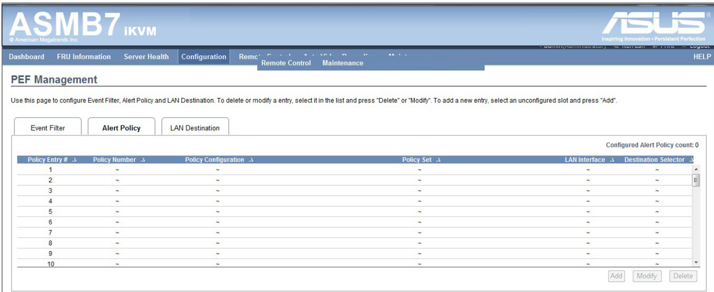
5. Generator ID configuration 部分：
- 勾选 Generator ID Data 项目用 RAW 数据填充 Generator ID。
- Generator ID 1 区域用于设置 raw generator ID1 数据。
- Generator ID 2 区域用于设置 raw generator ID2 数据。



在 RAW 数据的区域，用“0x”设置十六进制值前缀。

Alert Policy 标签页

此页用于设置 Alert Policy 与 LAN destination。您可以在此页面中添加、删除或修改条目。



PEF Management - Alert Policy 标签页说明如下。

1. Policy Entry #：显示新设置的 Policy 条目（只读）编号。
2. Policy Number：显示设置的 Policy 编号。
3. Policy Configuration：开启或关闭 Policy 设置。
4. Policy Set：从此列表中选择任一 Policy 设置。

   0 - 总是发送警报至此目的地。

   1 - 若发送警报至前一个目的地成功，不需发送警报至此目的地。继续执行这个 Policy 设置中的下一个条目。

   2 - 若发送警报至前一个目的地成功，不需发送警报至此目的地。继续执行这个 Policy 设置中的其他条目。

   3 - 若发送警报至前一个目的地成功，不需发送警报至此目的地。继续执行这个 Policy 设置中针对不同通道的下一个条目。

   4 - 若发送警报至前一个目的地成功，不需发送警报至此目的地。继续执行这个 Policy 设置中针对不同目的地类型的下一个条目。
5. Channel Number：从可用的通道列表中选择一个特定的通道。
6. Destination Selector：从已设置的目的地列表中选择一个特定的目的地。



进入 Configuration -> PEF -> LAN Destination 设置 LAN Destination。

7. Add：保存新的警报规则并返回 Alert Policy 列表。
8. Modify：修改已存在的条目。
9. Cance：取消更改并返回 Alert Policy 列表。

步骤：

Add Alert Policy entry

Policy Entry #	1
Policy Number	1
Policy Configuration	☐ Enable
Policy Set	0
LAN Interface	DM_LAN1
Destination Selector	1
Alert String	☐ Event Specific
Alert String Key	0

Add Cancel

1. 在 Alert Policy 标签页中，选择您要设置警报规则的插槽。例如，在 Event Filter Entry 页面中，若您选择了第 4 条 Alert Policy，您必须设置第四插槽（Policy 编号为 4 的插槽）。
2. 选择插槽并点击 Add 打开 Add Alert Policy Entry 页面。
3. Policy Entry # 为只读区域。
4. 从列表中选择 Policy Number。
5. 在 Policy Configuration 区域，若您想开启规则设置则勾选 Enable。
6. 在 Policy Set 区域，从列表中选择任一 Policy 设置。
7. 在 Channel Number 区域，从可用的通道列表中选择特定的通道。
8. 在 Destination Selector 区域，从已设置的目的地列表中选择特定的目的地。

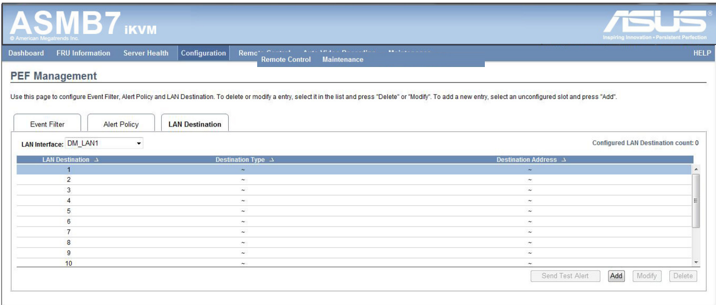


进入 Configuration -> PEF -> LAN Destination 设置 LAN Destination。例如，在 Alert Policy Entry 页面中，若您选择了第 4 个目的地，您必须设置第四插槽（LAN Destination 编号为 4 的插槽）。

9. 在 Alert String 区域，勾选 Event Specific。
10. 在 Alert String Key 区域，选择任一设置值，用来查看为这个 Alert Policy 发送的 Alert String。
11. 点击 Add 保存新的警报规则并返回 Alert Policy 列表。
12. 点击 Cancel 取消更改并返回 Alert Policy 列表。
13. 在 Alert Policy 列表中，要更改设置，先选择要更改的插槽，然后点击 Modify。
14. 在 Modify Alert Policy Entry 页面中，进行必要的更改，然后点击 Modify。
15. 在 Alert Policy 列表中，要删除设置， 先选择插槽，然后点击 Delete。

PEF 管理 LAN Destination 设置页面

此页面用来设置 Event filter、Alert Policy 与 LAN destination。设置页面如下图所示。



PEF Management – LAN Destination 标签页说明如下。

1. LAN Destination： 显示新设置条目（只读）的目的地编号。
2. Destination Type：目的地类型可以是一个 SNMP Trap 或一个 Email 提醒。若是 Email 提醒，需要设置 3 项内容 - 目的地 Email 地址、主题与内容正文。另外还需要添加 SMTP 服务器信息 - 进入 Configuration -> SMTP 进行设置。若是 SNMP Trap，只需设置目的地 IP 地址。
3. Destination Address：若目的地类型为 SNMP Trap，输入将收到警报的系统 IP 地址。目的地地址支持以下格式：

   - IPv4 地址格式
   - IPv6 地址格式

   若目的地类型为 Email 提醒，输入将收到电子邮件的 Email 地址。
4. Subject & Message：若目的地类型为 Email 提醒，则必须设置此项目。发送的邮件将会包含特定主题与正文内容。
5. Add：保存新的 LAN 目的地并返回 LAN Destination 列表。
6. Cancel：取消更改并返回 LAN Destination 列表。

步骤：

Add LAN Destination entry

LAN Channel Number	1
LAN Destination	1
Destination Type	Snmp Trap
Destination Address	
Username	anonymous
Message	

Add　Cancel

1. 在 LAN Destination 标签页中，选择您要设置的插槽。此插槽必须与您在 Alert Policy Entry- Destination Selector 中选择的相同。例如，您在 Alert Policy 标签页的 Alert Policy Entry 页面中将 Destination Selector 选择为 4，那么您必须设置 LAN Destination 页面的第四插槽。
2. 选择插槽并点击 Add 打开 Add LAN Destination Entry 页面。
3. 在 LAN Destination 区域，会显示新设置条目的目的地，且为只读。
4. 在 Destination Type 区域选择类型。
5. 在 Destination Address 区域，输入目的地地址。



注意：若目的地类型为 Email 提醒，输入将收到电子邮件的 Email 地址。

6. 从用户列表中选择 User Name。
7. 在 Subject 区域，输入主题。
8. 在 Message 区域，输入内容。
9. 点击 Add 保存新的 LAN 目的地并返回 LAN Destination 列表。
10. 点击 Cancel 取消更改并返回 LAN Destination 列表。
11. 在 LAN Destination 标签页中，要更改设置，先选择要更改的行，然后点击 Modify。
12. 在 Modify LAN Destination Entry 页面中，进行必要的更改，然后点击 Modify。
13. 在 LAN Destination 标签页中，要删除设置， 先选择插槽，然后点击 Delete。

4.4.9 RADIUS

此页面用来开启或关闭 RADIUS 验证，并输入所需信息来访问 RADIUS 服务器。

ASMB7 iKVM
Dashboard | FRU Information | Server Health | Configuration | Remote Control | Auto Video Recording | Maintenance | HELP

RADIUS Settings

Check the box below to enable RADIUS authentication and enter the required information to access the RADIUS server. Press the Save button to save your changes.

RADIUS Authentication: Enable
Port: 1812
Time Out: 3 seconds
Server Address
Secret

4.4.10 远程会话（Remote Session）

Remote Session 页面用来开启或关闭 KVM 或重定向会话时的数据加密。

ASMB7 iKVM
Dashboard | FRU Information | Server Health | Configuration | Remote Control | Auto Video Recording | Maintenance | HELP

Configure Remote Session

The following options are to enable or disable encryption on KVM or Media data for the next redirection session.

KVM Encryption: Enable
Media Encryption: Enable
Virtual Media Attach Mode: Attach

Save | Reset

1. KVM Encryption：为下一个重定向会话开启/关闭 KVM 数据加密。
2. Media Encryption：为下一个重定向会话开启/关闭媒体数据加密。
3. Virtual Media Attach Mode：有两种模式可用。
   - Attach - 开启后立即连接虚拟媒体至服务器。（此项目供本地 F/W 更新使用）
   - Auto Attach - 仅当虚拟媒体会话开启时连接虚拟媒体至服务器。
4. Save：保存当前更改。

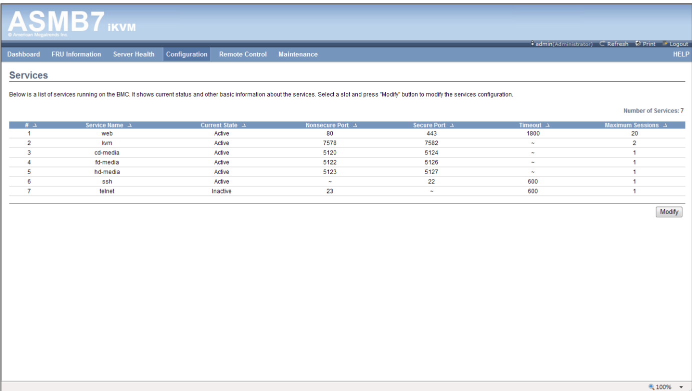


若出现任何问题，它将自动关闭当前存在的 KVM 或虚拟媒体会话的远程重定向。

5. Reset：重置更改的内容。

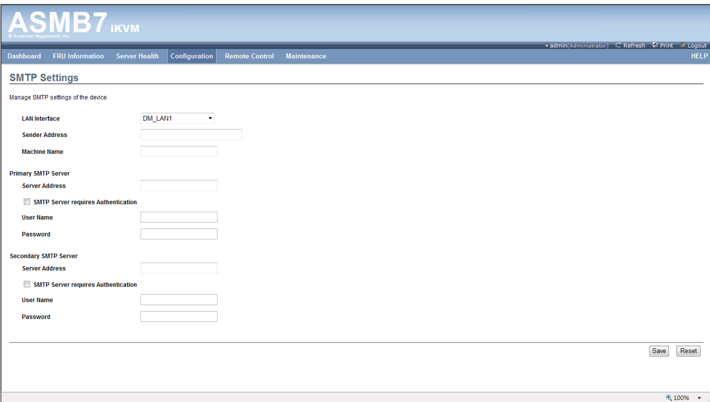
4.4.11 服务（Services）

此页面中列出了在 BMC 上运行的服务。显示服务的当前状态和其他基本信息。点击【Modify】修改服务设置。



4.4.12 SMTP

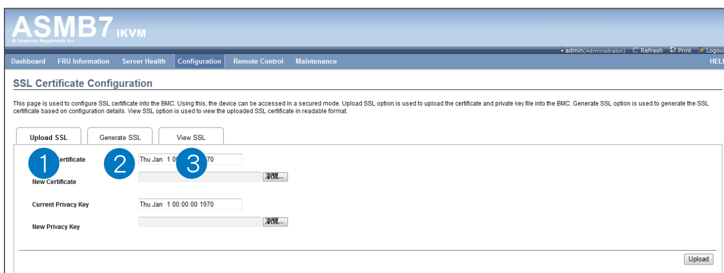
SMTP 页面用来设置 SMTP 邮件服务器。输入邮件服务器的 IP 地址，然后点击【Save】应用设置。



4.4.13 SSL

SSL（Secure Socket Layer）协议为 Netscape 所研发，用以保障网络服务器与浏览器之间的传输。协议使用第三方 CA（Certificate Authority）认证来识别传输的一端或两端。

从主菜单点击【Configuration】>【SSL】打开“SSL Certificate Configuration”页面。此页面有三个标签页。



1. 【Upload SSL】项目可用于上传证书与私人密钥文件至 BMC。
2. 【Generate SSL】项目用于依据设置信息生成 SSL证书。
3. 【View SSL】项目用于查看已上传的 SSL 证书。

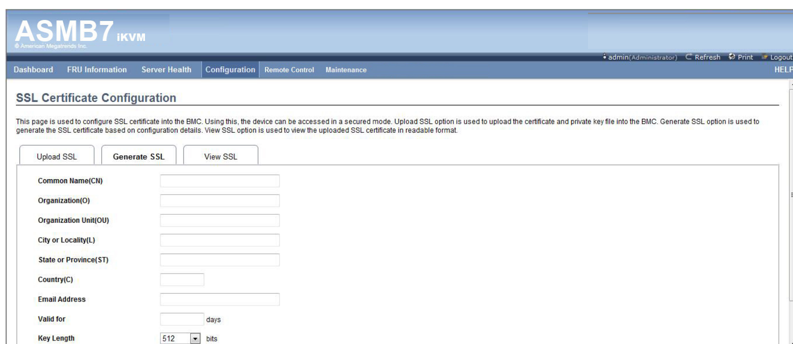


SSL Certificate Configuration – Upload SSL 标签页说明如下。

1. Current Certificate：显示当前证书信息（只读）。
2. New Certificate：要上传的证书，证书须为 pem 类型。
3. Current Privacy Key：显示当前隐私密钥信息（只读）。
4. New Privacy Key：新隐私密钥，须为 pem 类型。
5. Upload：上传 SSL 证书与隐私密钥至 BMC。



上传成功后，HTTPs 服务将会使用新上传的 SSL 证书开启。



SSL Certificate Configuration – Generate SSL 标签页说明如下。

1. Common Name(CN)：证书生成名称。
   - 最长 64 字符。
   - 不可使用特殊字符“#”与“$”。

2. Organization(O)：生成证书的组织者名称。

   - 最长 64 字符。

   - 不可使用特殊字符“#”与“$”。

3. Organization Unit(OU)：生成证书的组织者单位。

   - 最长 64 字符。

   - 不可使用特殊字符“#”与“$”。

4. City or Locality(L)：组织者城市（必填）。

   - 最长 64 字符。

   - 不可使用特殊字符“#”与“$”。

5. State or Province(ST)：组织者州/省（必填）。

   - 最长 64 字符。

   - 不可使用特殊字符“#”与“$”。

6. Country(C)：组织者国家代码（必填）。

   - 仅允许两个字符。

   - 不可使用特殊字符。

7. Email Address：组织者电子邮件地址（必填）。

8. Valid for：证书有效期。

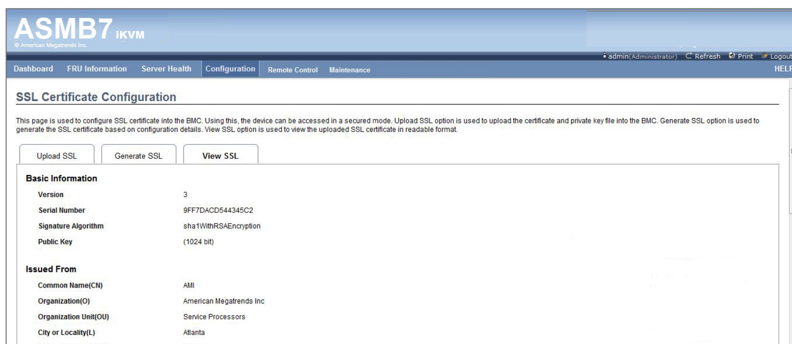
   - 有效期为 1 至 3650 天。

9. Key Length：证书位长。

10. Generate：生成新的 SSL 证书。



HTTPs 服务将会使用新上传的 SSL 证书开启。



SSL Certificate Configuration – Generate SSL 标签页说明如下。

1. Basic Information：此部分显示有关已上传 SSL 认证的基本信息，有以下内容：
    - Version
    - Serial Number
    - Signature Algorithm
    - Public Key
2. Issued From：此部分描述认证方信息。
    - Common Name(CN)
    - Organization(O)
    - Organization Unit(OU)
    - City or Locality(L)
    - State or Province(ST)
    - Country(C)
    - Email Address
3. Validity Information：此部分显示已上传认证的有效期。
    - Valid From
    - Valid To
4. Issued To：此部分显示认证方信息。
    - Common Name(CN)
    - Organization(O)

- Organization Unit(OU)
    - City or Locality(L)
    - State or Province(ST)
    - Country(C)
    - Email Address

步骤：

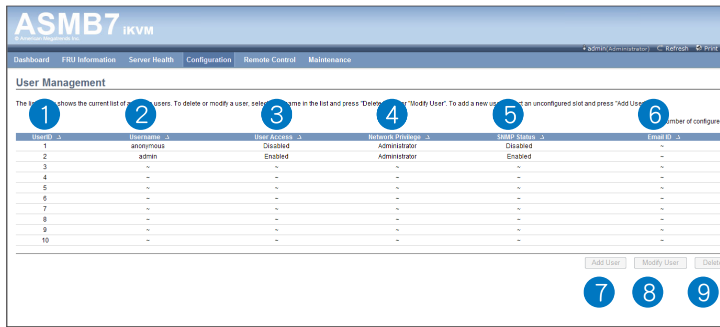
1. 点击 Upload SSL 标签页，浏览 New Certificate 与 New Privacy key。
2. 点击 Upload 上传新的证书与隐私密钥。
3. 在 Generate SSL 标签页中输入以下详细信息。
   - Common Name，证书生成名称
   - Name of the Organization，组织者名称
   - Overall Organization Section Unit，组织者单位
   - City or Locality，组织者城市
   - State or Province，组织者州（省）
   - Country，组织者国家
   - email address，组织者电子邮件地址
   - Valid For，证书有效时间
4. 选择 Key Length，设置证书的位元值。
5. 点击 Generate 生成证书。
6. 点击 View SSL标签页以用户可读的格式查看已上传 SSL 证书。



1. 上传或生成证书后，仅开启 HTTP 服务。
2. 您现在可以安全地访问您的 MegaRAC® SP，请使用以下链接：https://<您的 MegaRAC® SP 的 IP 地址>
3. 例如，若您的 MegaRAC® SP 的 IP 地址为 192.168.0.30，则输入 https://192.168.0.30
4. 请注意 <http> 后的 <s>。在访问 MegaRAC® SP 前，您必须接受证书。

4.4.14 用户（Users）

“User Management”页面中可查看服务器的当前用户插槽。您可以添加用户、修改或删除已存在的用户。“User Management”页面如下图所示。



1. User ID：显示用户的 ID 号码。注意：列表最多只能包含 10 个用户。
2. User Name：显示用户名称。
3. User Access：开启或关闭用户的存取权限。
4. Network Privilege：显示用户的网络存取权限。
5. SNMP Status：显示用户的 SNMP 状态是否为开启或关闭。
6. Email ID：显示用户的电子邮件地址。
7. Add User：添加一个新用户。
8. Modify User：修改已存在的用户。
9. Delete User：删除已存在的用户。

添加新用户：

1. 要添加一个新用户，选择一个空的插槽并点击【Add User】。
2. 在“User Name”区域输入用户的名称。
3. 在“Password”与“Confirm Password”区域，输入并确认您的密码。
4. 密码长度必须为 8~20 个字符，且不可使用空格。

5 开启或关闭 User Access Privilege.

6. 在“Network Privilege”区域，输入用户的网络权限：Administrator（管理员）、Operator（操作员）、User（用户）或 No Access（无权限）。

7. 勾选“SNMP Status”复选框为用户开启 SNMP 权限。注意：若 SNMP Status 开启，则必须设置密码。

8. 从“SNMP Access”下拉菜单中为用户选择 SNMP 存取层级：Read Only（只读）或 Read Write（读写）。

9. 从下拉列表中选择 SNMP 设置使用的 Authentication Protocol。注意：若 Authentication 协议改变，则必须设置密码。

10. 从“Privacy protocol”下拉菜单中选择 SNMP 设置使用的 Encryption algorithm。

11. 在“Email ID”区域，输入用户的电子邮件帐号。若用户忘记密码，新密码会通过邮件的方式寄至此电子邮件帐号。

    AMI-Format：此邮件格式的主题为“Alert from (your Hostname)”。此邮件的内容显示光标信息：光标类型与描述。

    Fixed-Subject Format：此格式会依据用户设置显示相关信息。您必须设置邮件警告的主题与信息。

12. 在“New SSK Key”区域，点击【Browse】并选择 SSH 密钥文件。注意：SSH 密钥文件应为 pub 类型。

13. 点击【Add】保存新用户并返回用户列表页面。

14. 点击【Cancel】取消修改并返回用户列表页面。

修改已有用户

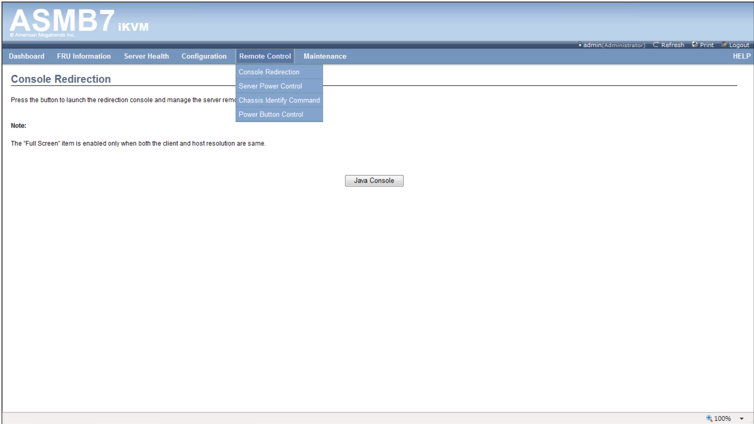
1. 从列表中选择一个用户，并点击【Modify User】。
2. 编辑需要的内容。
3. 要改变密码，开启【Change Password】项目。
4. 修改完成后，点击【Modify】返回用户列表页面。

删除已有用户

要删除用户，先从列表中选择用户，然后点击【Delete User】。

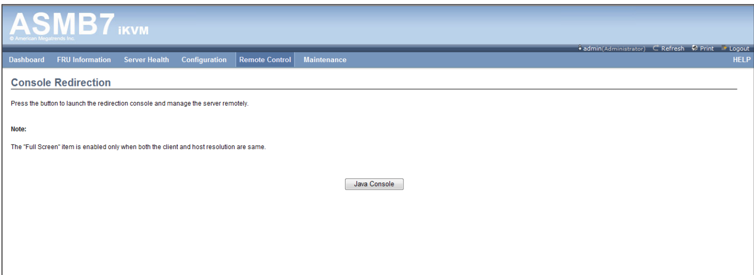
4.5 远程控制（Remote Control）

此部分允许您对服务器进行远程操作。点击每个选项开始进行设置。



4.5.1 Console Redirection

远程控制台应用程序，使用网页图形用户界面，可远程控制服务器的操作系统、使用屏幕、鼠标与键盘，以及重定向本地 CD/DVD、软盘与硬盘/USB 盘，如同这些设备是直接连接在服务器上。



浏览器设置

若开启 KVM，需解除对弹出窗口的阻止。若使用 Internet explorer，从设置中开启下载文件项目。

Java Console：

这是一个独立于操作系统的插件，可在 JRE 的辅助下在 Windows 与 Linux 中使用。客户端系统中需安装 JRE。您可以从以下链接安装 JRE：http://www.java.com/en/download/manual.jsp

两种方法开启 Java Console：

1. 打开 Dashboard 页面，在 Remote control 部分点击 Launch for Java Console。
2. 打开 Remote Control > Console Redirection 页面，点击 Java Console。

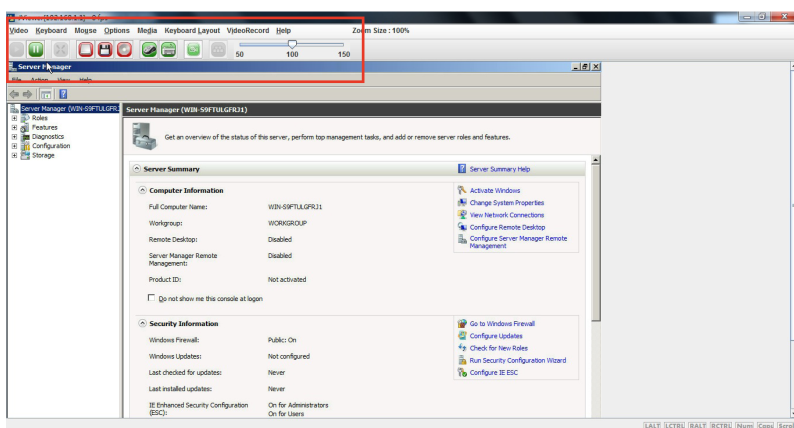
将从 BMC 下载 .jnlp 文件。

要开启 .jnlp 文件，使用适当的 JRE 版本（Javaws）下载完成后，Console Redirection 窗口开启。

Console Redirection 主菜单包含以下项目：

- 视频（Video）
- 键盘（Keyboard）
- 鼠标（Mouse）
- 选项（Options）
- 媒体（Media）
- 键盘概观（Keyboard Layout）
- 帮助（Help）

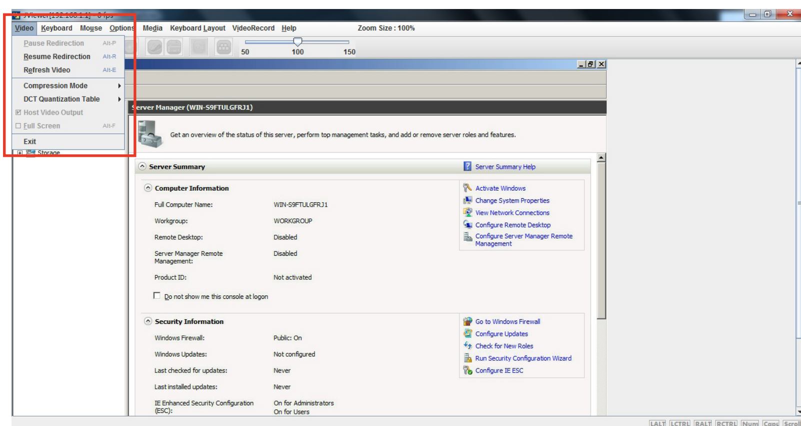
关于这些菜单的详细说明请参考以下部分。



视频（Video）

此菜单包含以下子项目：

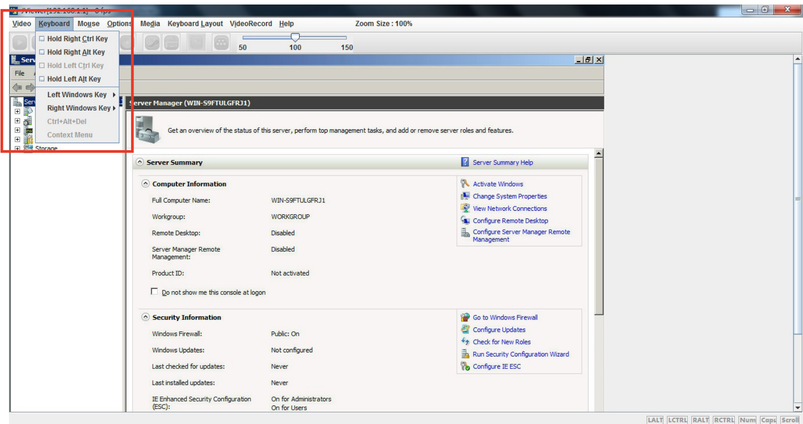
1. Pause redirection：此项目用来暂停 Console Redirection。
2. Resume Redirection：此项目用来当会话暂停时重新开始 Console Redirection。
3. Refresh Video：此项目用来刷新 Console Redirection 窗口的显示内容。
4. Compression Mode：此项目用来设置 Console Redirection 中的视频压缩。建议设置为 YUV420。
5. DCT Quantization Table：此项目用来设置 Console Redirection 中的 DCT 量化。建议设置为“4”。
6. Host Video Output：若您开启此选项，服务器显示将为空白，但您可以在 Console Redirection 中查看屏幕。若您关闭此选项，显示将会回到服务器屏幕。
7. Full Screen：此项目用来以全屏方式（最大化）查看 Console Redirection。只有当客户端与主机的分辨率相同时此项目才可使用。
8. Exit：此项目用来退出 console redirection 画面。



键盘（Keyboard）

此菜单包含以下子项目：

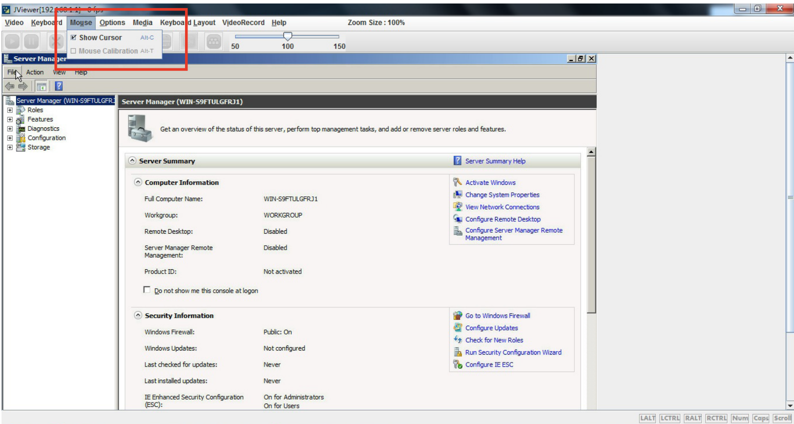
1. Hold Right Ctrl Key：在 Console Redirection 中此项目实现右边 <CTRL> 键功能。
2. Hold Right Alt Key：在 Console Redirection 中此项目实现右边 <ALT> 键功能。
3. Hold Left Ctrl Key：在 Console Redirection 中此项目实现左边 <CTRL> 键功能。
4. Hold Left Alt Key：在 Console Redirection 中此项目实现左边 <ALT> 键功能。
5. Left Windows Key：在 Console Redirection 中此项目实现左边 <WIN> 键功能。您也可以决定按键的方式：长按或按下后放开。
6. Right Windows Key：在 Console Redirection 中此项目实现右边 <WIN> 键功能。您也可以决定按键的方式：长按或按下后放开。
7. Alt+Ctrl+Del：此项目等同于当您在重定向时同时按下服务器上的 <CTRL>、<ALT> 与 <DEL> 键。
8. Context menu：在 Console Redirection 中此项目实现 context 菜单功能。



鼠标（Mouse）

1. Show Cursor：此项目用来显或隐藏远程客户端系统中的本地鼠标光标。
2. Mouse Calibration：只有当鼠标模式时此项目才可用。

在此步骤中，远程服务器上的鼠标阈值设置会被发现。本地鼠标的光标以红色显示，远程光标为远程视频画面中的一部分。两个光标都会在一开始便同步。请使用“+”或“-”键来改变阈值设置，直到两个光标不同步。请侦测第一个使两个光标不同步的阈值。侦测到后，使用 ‘ALT-T’ 保存阈值。



选项（Options）

Band width：Bandwidth Usage 项目用来调整频宽。您可以选择以下项目：

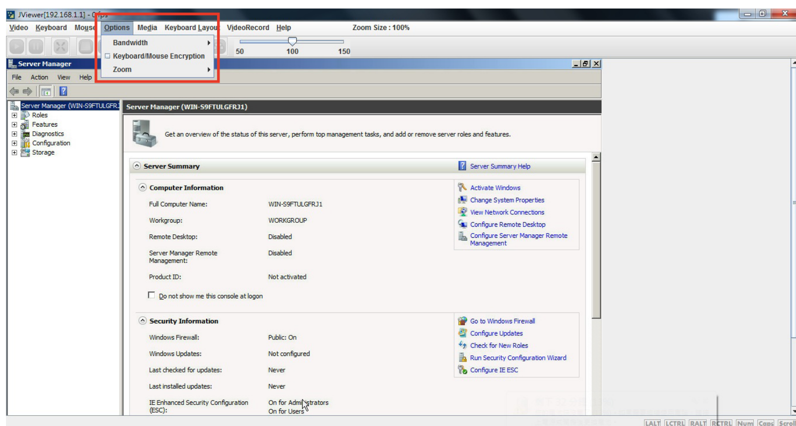
1. Auto Detect：此项目用来自动侦测客户端键盘分布，并依据侦测到的信息发送主要事件至主机。
2. 256 Kbps
3. 512 Kbps
4. 1 Mbps
5. 10 Mbps

Keyboard/Mouse Encryption：此项目用来加密键盘输入和鼠标移动。

缩放（Zoom):

只有当 Java Console 开启时此项目才可用。

1. Zoom In：放大画面尺寸。放大范围为 100% 到 150%，以 10% 为增量。
2. Zoom Out：缩小画面尺寸。缩小范围为 100% 到 50%，以 10% 为增量。



媒体（Media）

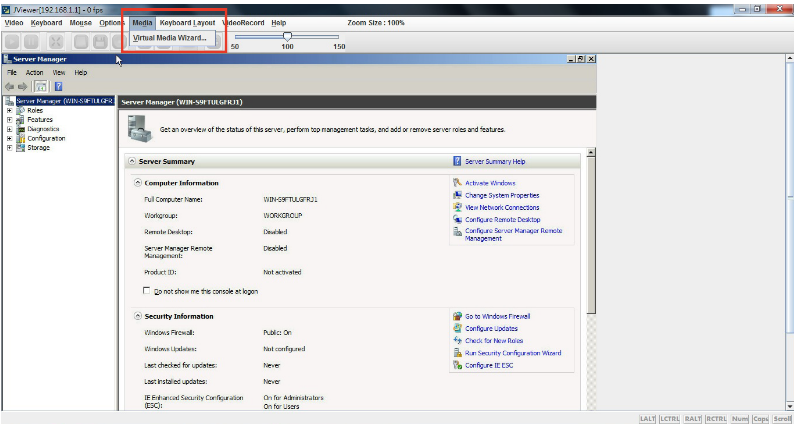
Virtual Media Wizard：

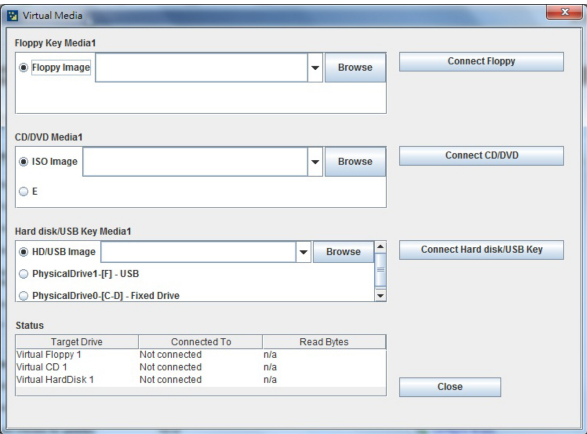
要添加或修改媒体，选择并点击 Virtual Media Wizard 按钮，然后会弹出一个名为“Virtual Media”的窗口，可以设置媒体。Virtual Media 画面如下图所示。

Floppy Key Media：此项目用来开始或停止物理软驱设备与软驱图片类型（如 img）的重定向。

CD/DVD Media：此项目用来开始或停止物理 DVD/CD-ROM 光驱与 cd 图片类型（如 iso）的重定向。

Hard disc/USB Key Media：此项目用来开始或停止 Hard Disk/USB 与 USB 图片（如 img）的重定向。



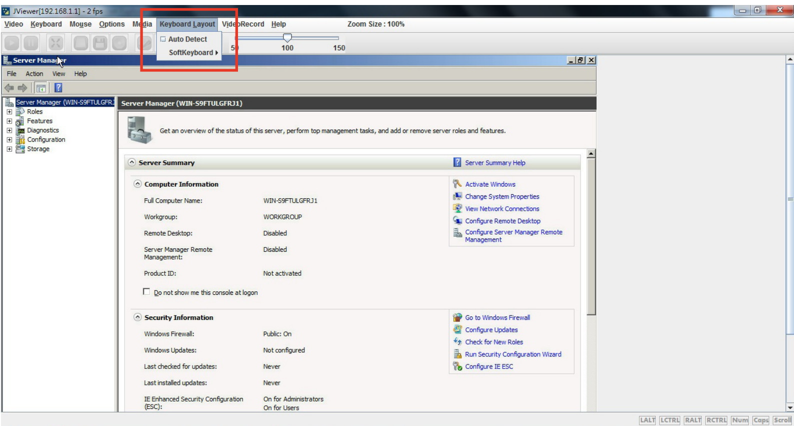


虚拟媒体向导

键盘概观（Keyboard Layout）

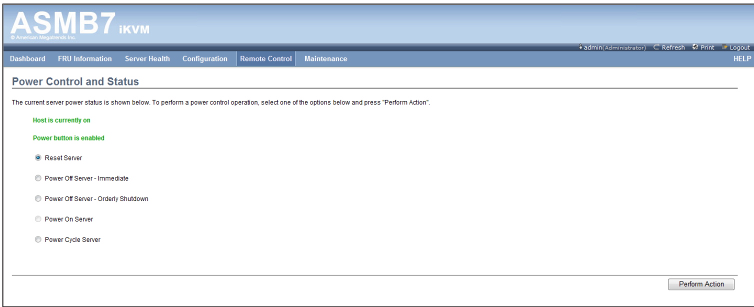
Auto Detect：此项目用来自动侦测键盘分布。语言自动支持 英语 - 法语 - 西班牙语 - 德语 - 日语。若客户端与主机的语言相同，那么除英语外，以上所有语言都必须选择此项目以避免输入错误。

Soft Keyboard：此项目用来选择键盘分布。屏幕中会显示一个如键盘一样的对话框。若客户端与主机的语言不同，那么除英语外，以上所有语言都必须在 JViewer 中的列表中选择适当的语言并使用软键盘以避免输入错误。注意：软键盘只适用于 JViewer 应用程序，并不适用于客户端系统。



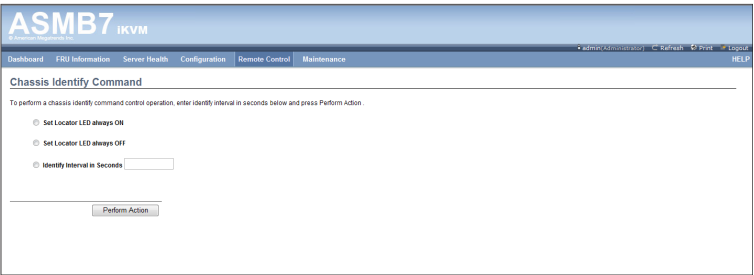
4.5.2 服务器电源管理（Server Power Control）

“Server Power Control”页面显示现在服务器电源状态，并允许您变更当前的设置。请选择您想要的项目，然后点击【Perform Action】执行选择的操作。



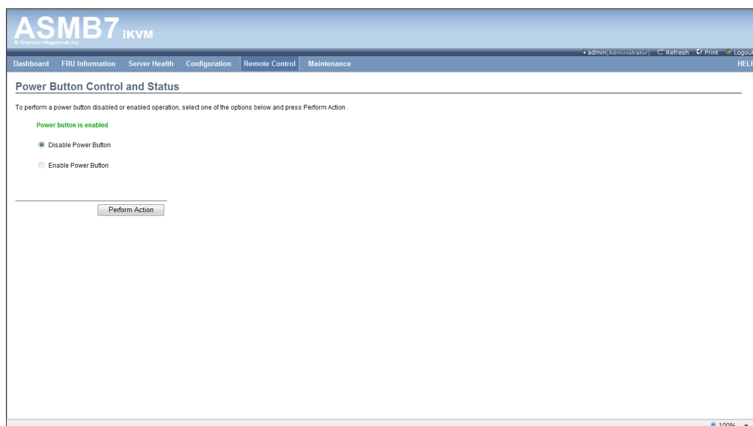
4.5.3 机箱识别指令（Chassis Identify Command）

在“Chassis Identify Command”页面中您可以执行控制机箱识别指令。点击【Perform Action】执行命令。



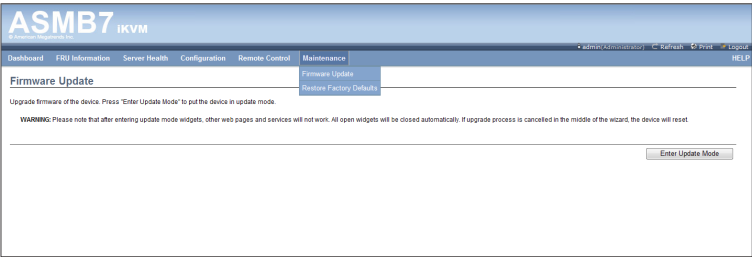
4.5.4 电源按钮（Power Button）

“Power Button”页面允许您开启或关闭电源按钮，然后点击【Perform Action】确认选择。



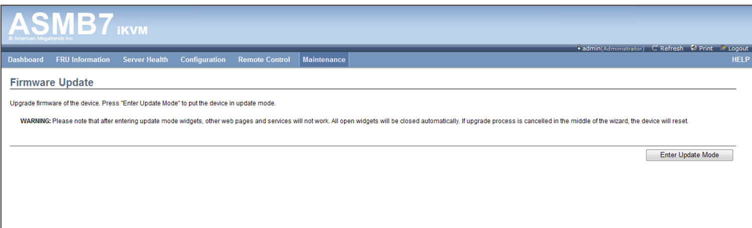
4.6 维护（Maintenance）

此部分用来为远程服务器进行固件升级。您也可以使用【Restore Factory Defaults】重置系统并使用【System Admnistrator】来开启或关闭访问权限、变更管理员帐户密码。



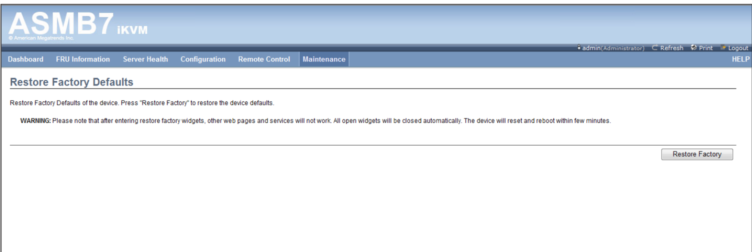
4.6.1 固件升级（Firmware Update）

此部分可进入升级模式并升级 ASMB7 的固件。请注意，进入升级模式 widget 后，其他网页与服务将停止运行。所有开启的 widget 将自动关闭。若升级过程在向导中途被取消，设备将重置。



4.6.2 恢复出厂默认设置

此部分用来恢复所有出厂默认设置。请点击【Restore Factory】进行恢复。



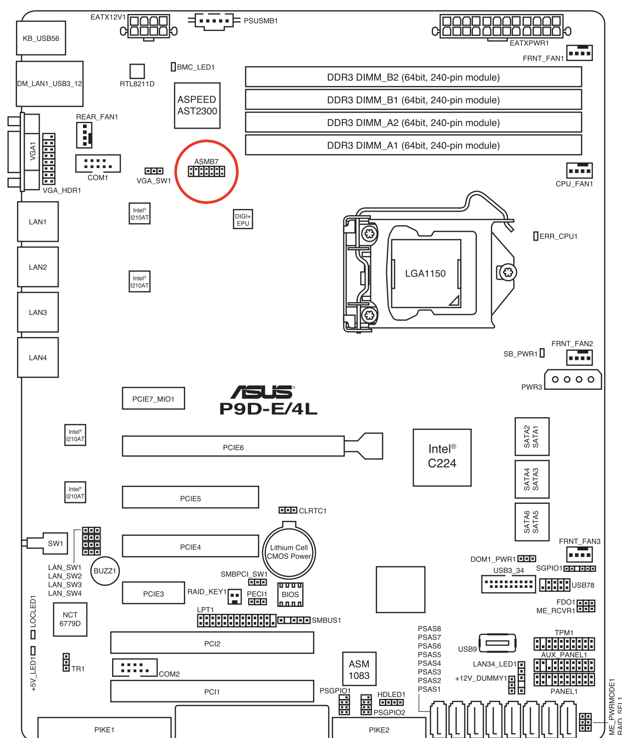
本章附录介绍了 BMC 与 LAN 接口在主板上的位置，并提供了在安装与使用管理卡的过程中出现的常见问题的解决方法。

参考信息 A

A.1 BMC 插座

华硕服务器主板支持具有底板管理控制器（Baseboard Management Controller，BMC）接口的 ASMB7-iKVM 远程管理卡。

BMC 插座的位置请参考下列图示。



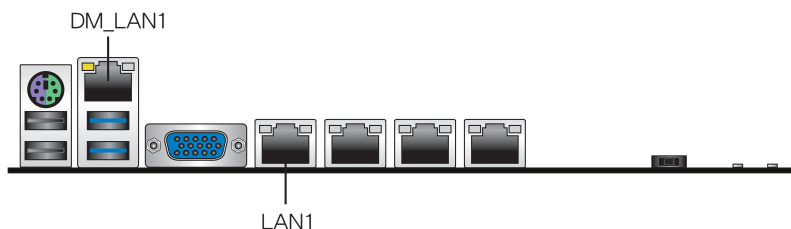


主板图示仅供参考，主板型号不同则外观也会不同。

A.2 LAN 接口

华硕服务器主板支持具有三个 LAN (RJ-45) 网络接口的 ASMB7-iKVM 远程管理卡：一个用于网络连接，另两个用于服务器管理。用于服务器管理的接口标示为 LAN1 与 DM_LAN1。您必须使用 LAN1 与 DM_LAN1 接口将远程服务器连接到本地 / 中心主机（直接 LAN 连接）或网络集线器或路由器。

LAN1 与 DM_LAN1 接口的位置请参考下列图示。





LAN1 与 DM_LAN1 的具体位置请参考主板用户手册。

A.3 疑难解决



疑难解决部分提供了一些在您安装 / 使用华硕 ASMB7-iKVM 管理卡时常见问题的解决方法，帮助您轻松解决问题。若尝试了此部分的方法仍未解决问题或有其他问题，请联系技术支持部门。

问题	解决方法
本地/ 中心服务器无法连接到 ASMB7-iKVM 远程管理卡	1. 检查网线是否正确插入 LAN 接口。 2. 请确认远程与本地 / 中心服务器的 IP 地址在同一个子网内。（请参考第二章的说明）在本地 / 中心服务器上尝试“ping xx.xx.xx.xx”（远程服务器 IP），并确认远程服务器可回复 ping 请求。 3. 检查 IP 源是否设置为 [DHCP]。若设为 [DHCP]，您无法设置 IP 地址。
所有 SEL（系统事件日志）无法显示	最大 SEL 数为 900 个事件。
SEL（系统事件日志）中显示的的日期 / 时间不正确	请参考 4.4.9 的说明，检查时区是否设置错误。
ASMB7-iKVM 在防火墙环境下无法连接网络	请 MIS 在防火墙中添加以下接口数： 5123（虚拟软驱）（TCP） 5120（虚拟 CDROM）（TCP） 623（IPMI）（TCP & UDP） 80（HTTP）（TCP） 7578（iKVM）（TCP） 443（HTTPs）（TCP） 161（SNMP）（UDP）
Java 重定向画面无法正常显示	点击【Refresh Page】键刷新重定向屏幕。



ASMB JAVA console 仅适用于内置的显卡，在其他的视频卡上可能无法正常显示。

A.4 监控器表

内存 ECC

编号	名称	类型	类型编码	设置值或事件类型	事件日期 3
0xD1	CPU1_ECC1	Memory ECC Sensor	0x0C	Discrete(0x6F) 0x01: Correctable ECC 0x02: Uncorrectable ECC 0x40: Presence detected	0x00: DIMM_A1, 0x01: DIMM_A2, 0x02: DIMM_A3, 0x03: DIMM_A4, 0x04: DIMM_B1, 0x05: DIMM_B2, 0x06: DIMM_B3, 0x07: DIMM_B4, 0x08: DIMM_C1, 0x09: DIMM_C2, 0x0A: DIMM_C3, 0x0B: DIMM_C4, 0x0C: DIMM_D1, 0x0D: DIMM_D2, 0x0E: DIMM_D3, 0x0F: DIMM_D4
0xD2	CPU1_ECC2	OEM Memory ECC Sensor (For Intel DP platform only -- ASUS Z8 series server MB; -E6 server system)	0xC1	Discrete(0x6F) 0x01: Read ECC error 0x02: ECC Error occurred on a scrub 0x04: Write Parity Error 0x08: Error in Redundant memory 0x10: Sparing Error 0x20: Memory access out of Range 0x40: Address Parity Error 0x80: Byte Enable Parity	0x00: DIMM_A1, 0x01: DIMM_A2, 0x02: DIMM_A3, 0x03: DIMM_A4, 0x04: DIMM_B1, 0x05: DIMM_B2, 0x06: DIMM_B3, 0x07: DIMM_B4, 0x08: DIMM_C1, 0x09: DIMM_C2, 0x0A: DIMM_C3, 0x0B: DIMM_C4, 0x0C: DIMM_D1, 0x0D: DIMM_D2, 0x0E: DIMM_D3, 0x0F: DIMM_D4
0xD3	CPU2_ECC1	Memory ECC Sensor	0x0C	Discrete(0x6F) 0x01: Correctable ECC 0x02: Uncorrectable ECC 0x40: Presence detected	0x00: DIMM_D1, 0x01: DIMM_D2, 0x02: DIMM_D3, 0x03: DIMM_D4, 0x04: DIMM_E1, 0x05: DIMM_E2, 0x06: DIMM_E3, 0x07: DIMM_E4, 0x08: DIMM_F1, 0x09: DIMM_F2, 0x0A: DIMM_F3, 0x0B: DIMM_F4, 0x0C: DIMM_G1, 0x0D: DIMM_G2, 0x0E: DIMM_G3, 0x0F: DMM_G4, 0x10: DIMM_H1, 0x11: DIMM_H2, 0x12: DIMM_H3, 0x13: DIMM_H4, 0x14: DIMM_C1, 0x15: DIMM_C2, 0x16: DIMM_C3, 0x17: DIMM_C4
0xD4	CPU2_ECC2	OEM Memory ECC Sensor (For Intel DP platform only -- ASUS Z8 series server MB; -E6 server system)	0xC1	Discrete(0x6F) 0x01: Read ECC error 0x02: ECC Error occurred on a scrub 0x04: Write Parity Error 0x08: Error in Redundant memory 0x10: Sparing Error 0x20: Memory access out of Range 0x40: Address Parity Error 0x80: Byte Enable Parity	0x00: DIMM_D1, 0x01: DIMM_D2, 0x02: DIMM_D3, 0x03: DIMM_D4, 0x04: DIMM_E1, 0x05: DIMM_E2, 0x06: DIMM_E3, 0x07: DIMM_E4, 0x08: DIMM_F1, 0x09: DIMM_F2, 0x0A: DIMM_F3, 0x0B: DIMM_F4, 0x0C: DIMM_G1, 0x0D: DIMM_G2, 0x0E: DIMM_G3, 0x0F: DMM_G4, 0x10: DIMM_H1, 0x11: DIMM_H2, 0x12: DIMM_H3, 0x13: DIMM_H4, 0x14: DIMM_C1, 0x15: DIMM_C2, 0x16: DIMM_C3, 0x17: DIMM_C4

Backplane HD

编号	名称	类型	类型编码	设置值或事件类型
0x68	Backplane1 HD1	Drive Slot	0x0D	Discrete(0x6F) 0x01: Drive Presence 0x02: Drive Fault 0x80: Rebuild
0x69	Backplane1 HD2	Drive Slot	0x0D	Discrete(0x6F) 0x01: Drive Presence 0x02: Drive Fault 0x80: Rebuild
0x6A	Backplane1 HD3	Drive Slot	0x0D	Discrete(0x6F) 0x01: Drive Presence 0x02: Drive Fault 0x80: Rebuild
0x6B	Backplane1 HD4	Drive Slot	0x0D	Discrete(0x6F) 0x01: Drive Presence 0x02: Drive Fault 0x80: Rebuild
0x6C	Backplane1 HD5	Drive Slot	0x0D	Discrete(0x6F) 0x01: Drive Presence 0x02: Drive Fault 0x80: Rebuild
0x6D	Backplane1 HD6	Drive Slot	0x0D	Discrete(0x6F) 0x01: Drive Presence 0x02: Drive Fault 0x80: Rebuild
0x6E	Backplane1 HD7	Drive Slot	0x0D	Discrete(0x6F) 0x01: Drive Presence 0x02: Drive Fault 0x80: Rebuild
0x6F	Backplane1 HD8	Drive Slot	0x0D	Discrete(0x6F) 0x01: Drive Presence 0x02: Drive Fault 0x80: Rebuild
0x78	Backplane2 HD1	Drive Slot	0x0D	Discrete(0x6F) 0x01: Drive Presence 0x02: Drive Fault 0x80: Rebuild
0x79	Backplane2 HD2	Drive Slot	0x0D	Discrete(0x6F) 0x01: Drive Presence 0x02: Drive Fault 0x80: Rebuild
0x7A	Backplane2 HD3	Drive Slot	0x0D	Discrete(0x6F) 0x01: Drive Presence 0x02: Drive Fault 0x80: Rebuild
0x7B	Backplane2 HD4	Drive Slot	0x0D	Discrete(0x6F) 0x01: Drive Presence 0x02: Drive Fault 0x80: Rebuild
0x7C	Backplane2 HD5	Drive Slot	0x0D	Discrete(0x6F) 0x01: Drive Presence 0x02: Drive Fault 0x80: Rebuild
0x7D	Backplane2 HD6	Drive Slot	0x0D	Discrete(0x6F) 0x01: Drive Presence 0x02: Drive Fault 0x80: Rebuild
0x7E	Backplane2 HD7	Drive Slot	0x0D	Discrete(0x6F) 0x01: Drive Presence 0x02: Drive Fault 0x80: Rebuild
0x7F	Backplane2 HD8	Drive Slot	0x0D	Discrete(0x6F) 0x01: Drive Presence 0x02: Drive Fault 0x80: Rebuild

电源

编号	名称	类型	类型编码	设置值或事件类型
0x81	PSU1 Temp	Temperature	0x01	Threshold(0x01) Upper Non-Critical - going high Upper Critital - going high
0x82	PSU1 Fan1	FAN	0x04	Threshold(0x01) Lower Non-critical - going low Lower Critital - going low
0x83	PSU1 Fan2	FAN	0x04	Threshold(0x01) Lower Non-critical - going low Lower Critital - going low
0x92	PSU1 Over Temp	Temperature	0x01	Discrete(0x07) 0x01: Transition to OK 0x10: Transition to Non-Critical from more severe 0x40: Transition to Non-Recoverable
0x93	PSU1 FAN Low	FAN	0x04	Discrete(0x07) 0x01: Transition to OK 0x10: Transition to Non-Critical from more severe
0x94	PSU1 AC	Power Supply	0x08	Discrete(0x6F) 0x01: Presence Detected 0x08: Power Supply input lost (AC/DC)
0x95	PSU1 Slow FAN1	FAN	0x04	Discrete(0x07) 0x01: Transition to OK 0x10: Transition to Non-Critical from more severe 0x40: Transition to Non-Recoverable
0x96	PSU1 Slow FAN2	FAN	0x04	Discrete(0x07) 0x01: Transition to OK 0x10: Transition to Non-Critical from more severe 0x40: Transition to Non-Recoverable
0x97	PSU1 PWR Detect	Power Supply	0x08	Discrete(0x6F) 0x01: Presence Detected 0x02: Power Supply Failure Detected
0x84	PSU2 Temp	Temperature	0x01	Threshold(0x01) Upper Non-Critical - going high Upper Critital - going high
0x85	PSU2 Fan1	FAN	0x04	Threshold(0x01) Lower Non-critical - going low Lower Critital - going low
0x86	PSU2 Fan2	FAN	0x04	Threshold(0x01) Lower Non-critical - going low Lower Critital - going low
0x9A	PSU2 Over Temp	Temperature	0x01	Discrete(0x07) 0x01: Transition to OK 0x10: Transition to Non-Critical from more severe 0x40: Transition to Non-Recoverable
0x9B	PSU2 FAN Low	FAN	0x04	Discrete(0x07) 0x01: Transition to OK 0x10: Transition to Non-Critical from more severe
0x9C	PSU2 AC Lost	Power Supply	0x08	Discrete(0x6F) 0x01: Presence Detected 0x08: Power Supply input lost (AC/DC)
0x9D	PSU2 Slow FAN1	FAN	0x04	Discrete(0x07) 0x01: Transition to OK 0x10: Transition to Non-Critical from more severe 0x40: Transition to Non-Recoverable
0x9E	PSU2 Slow FAN2	FAN	0x04	Discrete(0x07) 0x01: Transition to OK 0x10: Transition to Non-Critical from more severe 0x40: Transition to Non-Recoverable
0x9F	PSU2 PWR Detect	Power Supply	0x08	Discrete(0x6F) 0x01: Presence Detected 0x02: Power Supply Failure Detected

硬件监控

编号	名称	类型	类型编码	设置值或事件类型
0x31	CPU1 Temperature	Temperature	0x01	Threshold(0x01) Upper Non-critical - going high Upper Critical - going high
0x32	CPU2 Temperature	Temperature	0x01	Threshold(0x01) Upper Non-critical - going high Upper Critical - going high
0xCC	TR1 Temperature	Temperature	0x01	Threshold(0x01) Upper Non-critical - going high Upper Critical - going high
0xCD	TR2 Temperature	Temperature	0x01	Threshold(0x01) Upper Non-critical - going high Upper Critical - going high
0x34	VCORE1	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x35	VCORE2	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x36	+3.3V	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x37	+5V	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x38	+12V	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x39	+1.5V_ICH (For Intel DP platform only -- ASUS Z8 series server MB; -E6 server system)	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x3A	+1.1V_IOH (For Intel DP platform only -- ASUS Z8 series server MB; -E6 server system)	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x3B	+5VSB	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x3C	VBAT	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x3D	P1VTT (For Intel DP platform only -- ASUS Z8 series server MB; -E6 server system)	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x3E	+1.5V_P1DDR3 (For Intel platform only -- ASUS Z8 series server MB; -E6 server system)	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high

0x3F	P2VTT (For Intel DP platform only -- ASUS Z8 series server MB; -E6 server system)	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x40	+3.3VSB	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x41	+1.5V_P2DDR3 (For Intel DP platform only -- ASUS Z8 series server MB; -E6 server system)	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x42	P1DDR3 (For AMD platform only)	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x42	+1.5V (For Intel UP platform only)	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x43	P2DDR3 (For AMD platform only)	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x44	P1_+1.2V (For AMD platform only)	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x45	P2_+1.2V (For AMD platform only)	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x46	P1_VDDNB (For AMD platform only)	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x47	+1.8V (For AMD platform only)	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x48	+1.2V (For AMD platform only)	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x49	+1.1V (For AMD platform only)	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x4A	VTT (For AMD platform only)	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0xA0	CPU_FAN1	FAN	0x04	Threshold(0x01) Lower Non-critical - going low Lower Critital - going low
0xA1	CPU_FAN2	FAN	0x04	Threshold(0x01) Lower Non-critical - going low Lower Critital - going low

0xA2	FRNT_FAN1	FAN	0x04	Threshold(0x01) Lower Non-critical - going low Lower Critital - going low
0xA3	FRNT_FAN2	FAN	0x04	Threshold(0x01) Lower Non-critical - going low Lower Critital - going low
0xA4	FRNT_FAN3	FAN	0x04	Threshold(0x01) Lower Non-critical - going low Lower Critital - going low
0xA5	FRNT_FAN4	FAN	0x04	Threshold(0x01) Lower Non-critical - going low Lower Critital - going low
0xA6	REAR_FAN1	FAN	0x04	Threshold(0x01) Lower Non-critical - going low Lower Critital - going low
0xA7	REAR_FAN2	FAN	0x04	Threshold(0x01) Lower Non-critical - going low Lower Critital - going low
0xA8	FRNT_FAN5	FAN	0x04	Threshold(0x01) Lower Non-critical - going low Lower Critital - going low
0xA9	FRNT_FAN6	FAN	0x04	Threshold(0x01) Lower Non-critical - going low Lower Critital - going low
0xAA	FRNT_FAN7	FAN	0x04	Threshold(0x01) Lower Non-critical - going low Lower Critital - going low
0x4F	Chassis Intrusion	Physical Security (Chassis Intrusion)	0x05	Discrete(0x6F) 0x01: General Chassis Intrusion 0x02: Drive Bay Intrusion

华硕的联络信息

华捷联合信息（上海）有限公司 ASUS United Technology (Shanghai) CO., LTD（中国）

地址	上海市闵行莘庄工业区春东路508号
电话	+86-21-5442-1616
传真	+86-21-5442-0099
网址	http://www.asus.com.cn

技术支持

电话	+86-21-3704-4610 (800-820-6655)
在线支持	http://support.asus.com/techserv/techserv.aspx

华硕电脑公司 ASUSTeK COMPUTER INC.（亚太地区）

地址	台湾台北市北投区立德路15号 11259
电话	+886-2-2894-3447
传真	+886-2-2890-7798
E-mail	info@asus.com.tw
网址	http://www.asus.com.tw

技术支持

电话	+86-21-38429911
传真	+86-21-58668722 ext: 9101
在线支持	http://support.asus.com/techserv/techserv.aspx

ASUS COMPUTER INTERNATIONAL (美国)

地址	800 Corporate Way, Fremont, CA 94539, USA
传真	+1-510-608-4555
网址	http://usa.asus.com

技术支持

传真	+1-812-284-0883
一般支持	+1-812-282-2787
在线支持	http://support.asus.com/techserv/techserv.aspx

ASUS COMPUTER GmbH (德国/奥地利)

地址	Harkort Str. 21-23, 40880 Ratingen, Germany
传真	+49-2102-959911
网址	http://www.asus.de
在线联系	http://www.asus.de/sales

技术支持

电话	+49-1805-010923
传真	+49-2102-959911
在线支持	http://support.asus.com/techserv/techserv.aspx

DECLARATION OF CONFORMITY

Per FCC Part 2 Section 2. 1077(a)



Responsible Party Name: Asus Computer International

Address: 800 Corporate Way, Fremont, CA 94539.

Phone/Fax No: (510)739-3777/(510)608-4555

hereby declares that the product

Product Name : Management Card

Model Number : ASMB7-IKVM

Conforms to the following specifications:

☒ FCC Part 15, Subpart B, Unintentional Radiators

Supplementary Information:

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Representative Person's Name : **Steve Chang / President**

Signature :

Date : **Apr. 12, 2013**

Ver. 120601

EC Declaration of Conformity



We, the undersigned,

Manufacturer:	ASUSTeK COMPUTER INC.
Address, City:	4F, No. 150, LI-TE Rd., PEITOU, TAIPEI 112, TAIWAN
Country:	TAIWAN
Authorized representative in Europe:	ASUS COMPUTER GmbH
Address, City:	HARKORT STR. 21-23, 40880 RATINGEN
Country:	GERMANY

declare the following apparatus:

Product name :	**Management Card**
Model name :	**ASMB7-IKVM**

conform with the essential requirements of the following directives:

☒**2004/108/EC-EMC Directive**

☒ EN 55022:2010	☒ EN 55024:2010
☒ EN 61000-3-2:2006+A2:2009	☒ EN 61000-3-3:2008
☐ EN 55013:2001+A1:2003+A2:2006	☐ EN 55020:2007+A11:2011

☐**1999/5/EC-R &TTE Directive**

☐ EN 300 328 V1.7.1(2006-10)	☐ EN 301 489-1 V1.9.2(2011-09)
☐ EN 300 440-1 V1.6.1(2010-08)	☐ EN 301 489-3 V1.4.1(2002-08)
☐ EN 300 440-2 V1.4.1(2010-08)	☐ EN 301 489-4 V1.4.1(2009-05)
☐ EN 301 511 V9.0.2(2003-03)	☐ EN 301 489-7 V1.3.1(2005-11)
☐ EN 301 908-1 V5.2.1(2011-05)	☐ EN 301 489-9 V1.4.1(2007-11)
☐ EN 301 908-2 V5.2.1(2011-07)	☐ EN 301 489-17 V2.1.1(2009-05)
☐ EN 301 893 V1.6.1(2011-11)	☐ EN 301 489-24 V1.5.1(2010-09)
☐ EN 302 544-2 V1.1.1(2009-01)	☐ EN 302 326-2 V1.2.2(2007-06)
☐ EN 302 623 V1.1.1(2009-01)	☐ EN 302 326-3 V1.3.1(2007-09)
☐ EN 50360:2001	☐ EN 301 357-2 V1.4.1(2008-11)
☐ EN 62479:2010	☐ EN 302 291-1 V1.1.1(2005-07)
☐ EN 50385:2002	☐ EN 302 291-2 V1.1.1(2005-07)
☐ EN 62311:2008	

☐**2006/95/EC-LVD Directive**

☐ EN 60950-1 / A12:2011	☐ EN 60065:2002 / A12:2011

☐**2009/125/EC-ErP Directive**

☐ Regulation (EC) No. 1275/2008	☐ Regulation (EC) No. 278/2009
☐ Regulation (EC) No. 642/2009	

☒**2011/65/EU-RoHS Directive**

Ver. 130208

☒**CE marking**



(EC conformity marking)

Position : **CEO**

Name : **Jerry Shen**

Declaration Date: 12/04/2013

Year to begin affixing CE marking:2013

Signature :